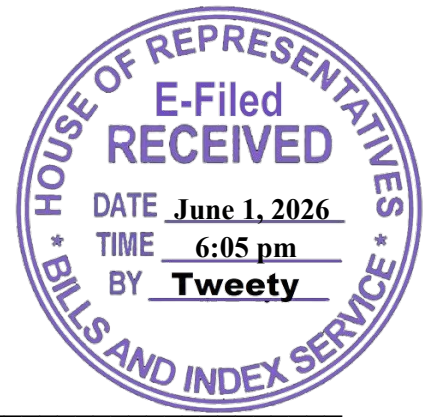


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session



COMMITTEE REPORT NO. 423

Submitted by the Committees on Information and Communications Technology and Appropriations on June 1, 2026.

Re : House Bill No. 9605

Recommending its approval in substitution of House Bills Numbered 9, 620, 660, 919, 1922, 2193, 2826, 3193, 3822, 4187, 4191, 4381, 5154, 5487, 5592, 6090, 6485, 6768, 6818, 7202, 7203, 7359, 7927, 8071, 8096, 8482, 8707 and 9197

Sponsors : Representatives Miguel Luis R. Villafuerte, Mikaela Angela B. Suansing, and Brian Poe

Mr. Speaker:

The Committee on Information and Communications Technology to which were referred House Bill No. 9, introduced by Reps. Ferdinand Martin G. Romualdez, Andrew Julian K. Romualdez, Jude A. Acidre, Eduardo R. Rama Jr., Maria Cristina C. Angeles, Antonio "Tonypet" T. Albano, Alyssa Michaela "Mica" M. Gonzales, Milagros Aquino-Magsaysay, Lani Mercado-Revilla, Karen Hope F. Garcia, Maria Rachel J. Arenas, Antonino B. Roman III, Steve Chiongbian Solon, Leody "Odie" F. Tarriela, Noel "Bong" N. Rivera, James "Jojo" Ang Jr., Ronaldo V. Puno, Ramon Jolo B. Revilla III, Ziaur-Rahman "Zia" Alonto Adiong, Javier Miguel Lopez Benitez, Antolin A. Oreta III, Claudine Diana D. Bautista-Lim, Jurdin Jesus M. Romualdo, Anna Victoria Veloso-Tuazon, Charisse Anne C. Hernandez and Ruth M. Sakaluran, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 620, introduced by Reps. Jurdin Jesus M. Romualdo and Noel "Bong" N. Rivera, entitled:

**“AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO
ADOPT AND IMPLEMENT ADEQUATE MEASURE TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND
INFRASTRUCTURE”;**

House Bill No. 660, introduced by Reps. Keith Micah "Atty. Mike" D.L. Tan, Iris Marie Demesa Montes, Noel "Bong" N. Rivera, Reynante U. Arrogancia, Gerardo "Gerryboy" J. Espina Jr. and Yevgeny Vincente B. Emano entitled:

**“AN ACT
INSTITUTIONALIZING POLICIES FOR A SECURE, TRUSTED, AND RELIABLE
CYBERSPACE, STRENGTHENING THE GOVERNANCE OF CYBERSECURITY,
ESTABLISHING FOR THE PURPOSE THE PHILIPPINE CYBERSECURITY COUNCIL,
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 919, introduced by Reps. Bernadette S. Barbers, Maria Cristina C. Angeles, and Noel "Bong" N. Rivera, entitled:

**“AN ACT
RATIONALIZING AND STRENGTHENING THE PHILIPPINE CYBERSECURITY
POSTURE AND CYBERCRIME RESPONSE”;**

House Bill No. 1922, introduced by Rep. Atty. Gerville "Jinky Bitrics" R. Luistro, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINE CYBERSECURITY COUNCIL
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 2193, introduced by Reps. Brian Poe, John Tracy F. Cagas, Bernadette G. Escudero, and Patrick Michael D. Vargas, entitled:

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

House Bill No. 2826, introduced by Reps. Miguel Luis R. Villafuerte, Vincenzo Renato Luigi R. Villafuerte, Tsuyoshi Anthony "Hori" G. Horibata, Terry L. Ridon, Faustino Michael Carlos T. Dy III, Ronaldo V. Puno, and Ferdinand "B1" L. Beltran, entitled:

**“AN ACT
AUTHORIZING THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE
AGAINST CYBERSECURITY THREATS AND INCIDENTS, CREATING THE
NATIONAL CYBERSECURITY AGENCY, DEFINING ITS POWERS AND FUNCTIONS,
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 3193, introduced by Reps. Emilio Bernardino L. Yulo and Maria Kristina Jihan B. Glepa, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 3822, introduced by Reps. Javier Miguel Lopez Benitez, Steve Chiongbian Solon, Alfredo "Albee" B. Benitez, Patrick Michael D. Vargas and John Tracy F. Cagas, entitled:

**“AN ACT
AUTHORIZING THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE
AGAINST CYBERSECURITY THREATS AND INCIDENTS, AND CREATING THE
NATIONAL CYBERSECURITY AGENCY, DEFINING ITS POWERS AND FUNCTIONS,
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 4187, introduced by Reps. Brian Poe, Bernadette G. Escudero and John Tracy F. Cagas entitled:

**“AN ACT
MANDATING CYBER MATURITY AND POSTURE ASSESSMENTS FOR ALL
GOVERNMENT AGENCIES AND OPERATORS OF CRITICAL INFRASTRUCTURE,
AND FOR OTHER PURPOSES”;**

House Bill No. 4191, introduced by Reps. Brian Poe and John Tracy F. Cagas entitled:

**“AN ACT
STRENGTHENING CYBERSECURITY STANDARDS FOR CRITICAL GOVERNMENT
AND PRIVATE INFRASTRUCTURE AND FOR OTHER PURPOSES”;**

House Bill No. 4381, introduced by Reps. Bryan B. Revilla, Lani Mercado-Revilla, Ramon Jolo B. Revilla III, Kristine Singson-Meehan and Maria Rachel J. Arenas, entitled:

**“AN ACT
AUTHORIZING THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE
AGAINST CYBERSECURITY THREATS AND INCIDENTS, AND CREATING THE
NATIONAL CYBERSECURITY AGENCY, DEFINING ITS POWERS AND FUNCTIONS,
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 5154, introduced by Reps. Yedda Marie K. Romualdez and Ma. Victoria Co-Pilar, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 5487, introduced by Reps. Juan Carlos "Arjo" C. Atayde and Ronaldo V. Puno, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 5592, introduced by Rep. Salvador A. Pleyto, entitled:

**“AN ACT
INSTITUTIONALIZING POLICIES FOR A SECURE, TRUSTED, AND RELIABLE
CYBERSPACE, STRENGTHENING THE GOVERNANCE OF CYBERSECURITY,
ESTABLISHING FOR THE PURPOSE THE PHILIPPINE CYBERSECURITY COUNCIL,
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 6090, introduced by Rep. Audrey Kay T. Zubiri, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY COUNCIL
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 6485, introduced by Reps. Edvic G. Yap and Eric Go Yap, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 6768, introduced by Rep. Eric L. Olivarez, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 6818, introduced by Rep. Alfred C. Delos Santos, entitled:

**“AN ACT
STRENGTHENING CYBERSECURITY AND CRITICAL INFRASTRUCTURE
PROTECTION, CREATING THE CYBERSECURITY AND INFRASTRUCTURE
PROTECTION COMMISSION, AND FOR OTHER PURPOSES”;**

House Bill No. 7202, introduced by Rep. Alexander Ty Pimentel, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINE CYBERSECURITY COUNCIL
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 7203, introduced by Rep. Alexander Ty Pimentel, entitled:

**“AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE INSTITUTIONS TO
ADOPT AND IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR
INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND
INFRASTRUCTURE”;**

House Bill No. 7359, introduced by Rep. Brian Raymund S. Yamsuan, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINE CYBERSECURITY COUNCIL
AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 7927, introduced by Rep. Christopherson "Coco" M. Yap, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREOF”;**

House Bill No. 8071, introduced by Rep. Jaime R. Fresnedi, entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
INTER-AGENCY COMMITTEE CREATED UNDER EXECUTIVE ORDER NO. 95 (S.
2019), RENAMING IT TO NATIONAL CYBERSECURITY COUNCIL, AND FOR OTHER
PURPOSES”;**

House Bill No. 8096, introduced by Rep. Ma. Nina Francesca P. Lacson and Julius Cesar "Jay" V. Vergara entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 8482, introduced by Rep. Ricardo S. Cruz Jr., entitled:

**“AN ACT
INSTITUTIONALIZING AND STRENGTHENING THE NATIONAL CYBERSECURITY
FRAMEWORK, AND ESTABLISHING THE PHILIPPINES CYBERSECURITY
COUNCIL AND APPROPRIATING FUNDS THEREFOR”;**

House Bill No. 8707, introduced by Reps. Jocelyn P. Tulfo and Ralph Wendel P. Tulfo, entitled:

**“AN ACT
ESTABLISHING THE PHILIPPINE CRITICAL INFORMATION INFRASTRUCTURE
PROTECTION FRAMEWORK, MANDATING CYBERSECURITY STANDARDS FOR
VITAL INDUSTRIES, PROVIDING CYBER-DEFENSE GRANTS FOR SMALL AND
MEDIUM ENTERPRISES, AND APPROPRIATING FUNDS THEREOF”;**

and House Bill No. 9197, introduced by Rep. Audrey Kay T. Zubiri, entitled:

**“AN ACT
REQUIRING CRITICAL INFORMATION INFRASTRUCTURE TO ADOPT AND
IMPLEMENT ADEQUATE MEASURES TO PROTECT THEIR INFORMATION AND
COMMUNICATIONS TECHNOLOGY (ICT) SYSTEMS AND INFRASTRUCTURE”.**

has considered the same and recommends that the attached House Bill No. 9605, entitled:

**“AN ACT
ESTABLISHING THE NATIONAL CYBERSECURITY AGENCY, STRENGTHENING
THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE, AND
PROVIDING FUNDS THEREFOR”**

be approved in substitution of House Bills Numbered 9, 620, 660, 919, 1922, 2193, 2826, 3193, 3822, 4187, 4191, 4381, 5154, 5487, 5592, 6090, 6485, 6768, 6818, 7202, 7203, 7359, 7927, 8071, 8096, 8482, 8707 and 9197 with Representatives Miguel Luis R. Villafuerte, Vincenzo Renato Luigi R. Villafuerte, Tsuyoshi Anthony "Hori" G. Horibata, Terry L. Ridon, Ferdinand Martin G. Romualdez, Andrew Julian K. Romualdez, Jude A. Acidre, Jurdin Jesus M. Romualdo, Keith Micah "Atty. Mike" D.L. Tan, Bernadette S. Barbers, Atty. Gerville "Jinky Bitrics" R. Luistro, Brian Poe, Emilio Bernardino L. Yulo, Javier Miguel Lopez Benitez, Bryan B. Revilla, Lani Mercado-Revilla, Ramon Jolo B. Revilla III, Yedda Marie K. Romualdez, Juan Carlos "Arjo" C. Atayde, Salvador A. Pleyto, Audrey Kay T. Zubiri, Edvic G. Yap, Eric Go Yap, Eric L. Olivarez, Alfred C. Delos Santos, Alexander Ty Pimentel, Brian Raymund S. Yamsuan, Christopherson "Coco" M. Yap, Jaime R. Fresnedi, Ma. Nina Francesca P. Lacson, Ricardo Jr. S. Cruz, Jocelyn P. Tulfo, Ralph Wendel P. Tulfo, Mikaela Angela B. Suansing, Nathaniel M. Oducado, Kristine Singson-Meehan, Ronaldo V. Puno, Yevgeny Vincente B. Emano, Maria Rachel J. Arenas, Alfredo "Albee" B. Benitez, Julius Cesar "Jay" V. Vergara Patrick Michael D. Vargas, Alyssa Michaela "Mica" M. Gonzales, Bernadette G. Escudero, Anna Victoria Veloso-Tuazon, Eduardo R. Rama Jr., Antonio L. Tinio, Agatha Paula Aguilar Cruz, Jose Manuel Tadeo "Chel" I. Diokno, Maria Cristina C. Angeles, Antonio "Tonypet" T. Albano, Milagros Aquino-Magsaysay, Karen Hope F. Garcia, Antonino B. Roman III, Steve Chiongbian Solon, Leody "Odie" F. Tarriela, Noel "Bong" N. Rivera, James "Jojo" Ang Jr., Ziaur-Rahman "Zia" Alonto Adiong, Antolin A. Oreta III, Claudine Diana D. Bautista-Lim,

Charisse Anne C. Hernandez, Ruth M. Sakaluran, Iris Marie Demesa Montes, Reynante U. Arrogancia, Gerardo "Gerryboy" J. Espina Jr., John Tracy F. Cagas, Faustino Michael Carlos T. Dy III, Ferdinand "B1" L. Beltran, Maria Kristina Jihan B. Glepa, Ma. Victoria Co-Pilar, Cheeno Miguel D. Almario, Jesus "Jess" R. Marquez, Maria Angela S. Garcia, Emmanuel L. Iway, Richelle Singson, Rebecca Maria Alcantara Ynares, Jose Manuel "JM" F. Lagdameo, Adrian E. Salceda, Jan "Atty. JP" DL. Padiernos, Angelo Marcos Barba, Dadah Kiram Ismula, Roman T. Romulo, Eulogio "Leo" R. Rodriguez, Edgar R. Erice, Tobias "Toby" M. Tiangco, Robert Nazal, Janette L. Garin, Jose "Bong" J. Teves, Jr., Albert S. Garcia, Jose C. Alvarez, Loreto S. Amante, Arnie B. Fuentebella, Dante S. Garcia, Alexandria "Queenie" Gonzales, Monique Yazmin Maria Q. Lagdameo, Ma. Christina Talavera Lopez, Romeo S. Momo Sr., Rufus B. Rodriguez, Ma. Isabel L. Sagarbarria, Joseph S. Tan, Amado Carlos A. Bolilia IV, Patricia C. Calderon, Timothy Joseph E. Cayton, Maximo Y. Dalog Jr., Felimon M. Espares, Nelson S. Legacion, Carlos Andes Loria, Dibu S. Tuan, Rolando M. Valeriano, Florabel C. Yatco, Arlyn P. Ayon, Elijah Rumbaoa San Fernando, Jan Franz Norbert Joselito A. Chan, Gerald Cloyd Alexis V. Galang, Atty. Jennifer "Karen" A. Lagbas and Linabelle Ruth R. Villarica as authors thereof.

Respectfully submitted,


MIKAEILA ANGELA B. SUANSING
Chairperson
Committee on Appropriations


MIGUEL LUIS R. VILLAFUERTE
Chairperson
Committee on Information and
Communications Technology

THE HONORABLE SPEAKER
HOUSE OF REPRESENTATIVES
Quezon City

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 9605

(In Substitution of House Bills Numbered 9, 620, 660, 919, 1922, 2193, 2826, 3193, 3822, 4187, 4191, 4381, 5154, 5487, 5592, 6090, 6485, 6768, 6818, 7202, 7203, 7359, 7927, 8071, 8096, 8482, 8707 and 9197)

Introduced by Representatives Miguel Luis R. Villafuerte, Vincenzo Renato Luigi R. Villafuerte, Tsuyoshi Anthony "Hori" G. Horibata, Terry L. Ridon, Ferdinand Martin G. Romualdez, Andrew Julian K. Romualdez, Jude A. Acidre, Jurdin Jesus M. Romualdo, Keith Micah "Atty. Mike" D.L. Tan, Bernadette S. Barbers, Atty. Gerville "Jinky Bitrics" R. Luistro, Brian Poe, Emilio Bernardino L. Yulo, Javier Miguel Lopez Benitez, Bryan B. Revilla, Lani Mercado-Revilla, Ramon Jolo B. Revilla III, Yedda Marie K. Romualdez, Juan Carlos "Arjo" C. Atayde, Salvador A. Pleyto, Audrey Kay T. Zubiri, Edvic G. Yap, Eric Go Yap, Eric L. Olivarez, Alfred C. Delos Santos, Alexander Ty Pimentel, Brian Raymund S. Yamsuan, Christopherson "Coco" M. Yap, Jaime R. Fresnedi, Ma. Nina Francesca P. Lacson, Ricardo Jr. S. Cruz, Jocelyn P. Tulfo, Ralph Wendel P. Tulfo, Mikaela Angela B. Suansing, Nathaniel M. Oducado, Kristine Singson-Meehan, Ronaldo V. Puno, Yevgeny Vincente B. Emano, Maria Rachel J. Arenas, Alfredo "Albee" B. Benitez, Julius Cesar "Jay" V. Vergara Patrick Michael D. Vargas, Alyssa Michaela "Mica" M. Gonzales, Bernadette G. Escudero, Anna Victoria Veloso-Tuazon, Eduardo R. Rama Jr., Antonio L. Tinio, Agatha Paula Aguilar Cruz, Jose Manuel Tadeo "Chel" I. Diokno, Maria Cristina C. Angeles, Antonio "Tonypet" T. Albano, Milagros Aquino-Magsaysay, Karen Hope F. Garcia, Antonino B. Roman III, Steve Chiongbian Solon, Leody "Odie" F. Tarriela, Noel "Bong" N. Rivera, James "Jojo" Ang Jr., Ziaur-Rahman "Zia" Alonto Adiong, Antolin A. Oreta III, Claudine Diana D. Bautista-Lim, Charisse Anne C. Hernandez, Ruth M. Sakaluran, Iris Marie Demesa Montes, Reynante U. Arrogancia, Gerardo "Gerryboy" J. Espina Jr., John Tracy F. Cagas, Faustino Michael Carlos T. Dy III, Ferdinand "B1" L. Beltran, Maria Kristina Jihan B. Glepa, Ma. Victoria Co-Pilar, Cheeno Miguel D. Almario, Jesus "Jess" R. Marquez, Maria Angela S. Garcia, Emmanuel L. Iway, Richelle Singson, Rebecca Maria Alcantara Ynares, Jose Manuel "JM" F. Lagdameo, Adrian E. Salceda, Jan "Atty. JP" DL. Padiernos, Angelo Marcos Barba, Dadah Kiram Ismula, Roman T. Romulo, Eulogio "Leo" R. Rodriguez, Edgar R. Erice, Tobias "Toby" M. Tiangco, Robert Nazal, Janette L. Garin, Jose "Bong" J. Teves, Jr., Albert S. Garcia, Jose C. Alvarez, Loreto S. Amante, Arnie B. Fuentesbella, Dante S. Garcia, Alexandria "Queenie" Gonzales, Monique Yazmin Maria Q. Lagdameo, Ma. Christina Talavera Lopez, Romeo S. Momo Sr., Rufus B. Rodriguez, Ma. Isabel L. Sagarbarria, Joseph S. Tan, Amado Carlos A. Bolilia IV, Patricia C. Calderon, Timothy Joseph E. Cayton, Maximo Y. Dalog Jr., Felimon M. Espares, Nelson S. Legacion, Carlos Andes Loria, Dibu S. Tuan, Rolando M. Valeriano, Florabel C. Yatco, Arlyn P. Ayon, Elijah Rumbaoa San Fernando, Jan Franz Norbert Joselito A. Chan, Gerald Cloyd Alexis V. Galang, Atty. Jennifer "Karen" A. Lagbas and Linabelle Ruth R. Villarica.

AN ACT
ESTABLISHING THE NATIONAL CYBERSECURITY AGENCY, STRENGTHENING THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE, AND PROVIDING FUNDS THEREFOR

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

CHAPTER I GENERAL PROVISIONS

SECTION 1. Short Title. – This Act shall be known as the “National Cybersecurity and Critical Information Infrastructure Protection Act of 2026”.

SEC. 2. Declaration of Policy. – The State recognizes the indispensable role of communication and information in nation-building and affirms its duty to safeguard personal data, information systems, and communications infrastructure within both the government and the private sector.

It is therefore declared the policy of the State to:

- a. Ensure a secure, trusted, and reliable cyberspace as a fundamental pillar of national security, economic prosperity, and social well-being;
- b. Protect critical information infrastructures (CII) from cyber threats, vulnerabilities, and attacks;
- c. Foster a culture of cybersecurity awareness, accountability, and shared responsibility among the government, the private sector, and the general public;
- d. Strengthen governance, coordination, and cooperation among all sectors in addressing cybersecurity concerns; and
- e. Promote the development of local cybersecurity talent, research, and technological innovation.

In pursuit of the foregoing policies, the State shall:

- a. Formulate and enforce effective cybersecurity policies;
- b. Establish a governance framework to ensure efficient coordination among government agencies and relevant sectors; and
- c. Institute proactive, timely, and appropriate responses to cybersecurity threats and incidents.

SEC. 3. Coverage. – This Act shall apply to:

- a. All national government agencies (NGAs), government-owned and controlled corporations (GOCCs), government financial institutions (GFIs), state universities and colleges (SUCs), and local government units (LGUs); except constitutional bodies and institutions that are granted fiscal and administrative autonomy in the performance of their constitutional and statutory mandates; *Provided, That* a cooperative mechanism

shall be established between regulatory agencies and industry leads such as but not limited to the Insurance Commission, Bangko Sentral ng Pilipinas (BSP), Securities and Exchange Commission (SEC), National Telecommunications Commission (NTC), Energy Regulatory Commission, to ensure the effective enforcement of the provisions of this Act;

- b. All CII owners and operators, whether public or private; *Provided*, That supervised institutions under regulatory agencies' supervision and regulation shall continue to be governed by applicable rules and regulations issued by said agencies in the exercise of their supervisory and regulatory authority;
- c. All entities providing cybersecurity products, services, or solutions to government or CII operators;
- d. All persons, natural or juridical, whose activities affect or are affected by the cybersecurity of Philippine cyberspace; and
- e. Cybersecurity matters with cross-border or transnational dimensions affecting Philippine interests.

No provision of this Act shall be interpreted to diminish, impair, or supersede the fiscal and administrative autonomy of government entities and constitutional bodies. Furthermore, this Act expressly preserves the full regulatory authority and supervisory powers of regulatory agencies over the institutions and entities within their respective jurisdictions.

SEC. 4. Interpretation. – In case of doubt, the provisions of this Act, including its implementing rules and regulations and any subsequent issuance by the implementing agency, shall be construed in a manner that accords the highest respect for human dignity, human rights, and individual privacy.

SEC. 5. Definition of Terms. – As used in this Act:

- a. *Computer emergency response team (CERT)* refers to a specialized unit responsible for providing services and support for the prevention, detection, handling, and coordination of the response and recovery from computer security incidents like malware infections, cyberattacks, and data breaches.
- b. *Computer system* refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output, and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage devices or

- media, both physical and virtual.
- c. *Confidentiality* refers to property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- d. *Critical information infrastructure (CII)* refers to the computer systems or networks, whether physical or virtual, and/or the computer programs, computer data, and/or traffic data that are vital to this country that the incapacity, destruction, or interference with such systems and assets would have a debilitating impact on security, national or economic security, national health and safety, or any combination of those matter.
- e. *Critical infrastructure (CI)* refers to any public service that owns, uses, or operates systems and assets, whether physical or virtual, vital to the Republic of the Philippines, the incapacity or destruction of such systems or assets would have a detrimental impact on national security, including telecommunications and such other vital services as may be declared by the President of the Philippines.
- f. *Chief Information Officer (CIO)* refers to a senior officer responsible for the development, planning, and implementation of the government entity's information systems strategic plan (ISSP) or information and communications technology (ICT) plan, and management of the agency's ICT systems, platforms, and applications.
- g. *Chief Information Security Officer (CISO)* refers to the official, designated by a covered entity, to lead its cybersecurity program and serve as liaison to the National Cybersecurity Agency (NCSA). The CISO shall be responsible for ensuring; (1) adherence to prescribed standards, (2) enhancement of the organization's information security capabilities, and (3) fulfillment of reporting obligations.
- h. *Covered entities* refer to organizations, business, or public offices that fall under the mandatory jurisdiction of specific regulatory bodies, laws, or audit requirements, in this case, falling under this Act and the NCSA.
- i. *Cryptographic primitive or crypto-primitive* refers to a low-level cryptographic algorithm used as a basic building block for higher-level cryptographic algorithms.
- j. *Cybercrime* refers to illegal activities conducted within the cyberspace. It involves activities violating laws and regulations such as the Cybercrime Prevention Act (Republic Act No. 10175, as amended).
- k. *Cybersecurity* refers to the organization and collection of resources, processes, and structures to preserve confidentiality, integrity, availability, non-repudiation, authenticity, privacy and safety in cyberspace.
- l. *Cyberspace* refers to a complex environment emerging from the interaction of people,

- 1 software, and services on the internet by means of technology devices and networks
2 connected to it, which does not exist in any physical form.
- 3 m. *Defense-CERT* refers to the national coordinating CERT for AFP-CERTS and state
4 sponsored cybersecurity incidents.
- 5 n. *Government computer emergency response team (GCERT)* refers to a specialized
6 trusted team within a government agency that manages, coordinates, and responds to
7 cybersecurity incidents, vulnerabilities, and threats.
- 8 o. *Information and communications technology (ICT)* refers to the totality of electronic
9 means to access, create, collect, store, process, receive, transmit, present, regulate,
10 and disseminate information.
- 11 p. *Information security* refers to the protection of information and systems from
12 unauthorized access, use, disclosure, disruption, modification, or destruction in order to
13 provide confidentiality, integrity, and availability.
- 14 q. *Integrity of information* refers to the assurance that information and systems are protected
15 against unauthorized modification.
- 16 r. *National computer emergency response team (NCERT)* refers to a unit under the
17 National Cybersecurity Agency responsible for performing CERT functions and
18 coordination among all CERTs. It is the primary coordinating center for all CERTs.
- 19 s. *National cyber intelligence network (NCIN)* refers to the inter-agency network managed
20 by the National Intelligence Coordinating Agency (NICA) responsible for the collection,
21 fusion, analysis, coordination and dissemination of strategic and operational cyber
22 intelligence concerning cyber threats to national security, counterintelligence in
23 cyberspace, and the attribution of state-sponsored cyber-attacks.
- 24 t. *National Security Operations Center (NSOC)* refers to an operations center housed
25 within the NCSA for centralized monitoring, threat detection, and incident response for
26 government agencies to enhance national cybersecurity. It shall monitor critical
27 information assets in cyberspace and conduct baseline assessment of government
28 agencies' cybersecurity posture.
- 29 u. *Non-repudiation* refers to the ability to prove the occurrence of a claimed event or action
30 and its originating entities.
- 31 v. *Organization computer emergency response team (ORG-CERT)* refers to responds to
32 cybersecurity incidents within an organization, regardless of their complexity or
33 criticality, while other coordinating CERTS such as the NCERT or SCERT, shall provide
34 specialist support and information to the organization CERT.

- 1 w. *Public Key Infrastructure (PKI)* refers to a set of policies, processes, server platforms,
2 software and workstations used for the purpose of administering certificates and public-
3 private key pairs, including the ability to issue, maintain, and revoke public key
4 certificates. The PKI includes the hierarchy of certificate authorities that allow for the
5 deployment of digital certificates that support encryption, digital signature and
6 authentication to meet business and security requirements.
- 7 x. *Privacy* refers to an individual's rights to exercise control over the collection, access,
8 use and disclosure of his or her personal information held by the government or the
9 private sector.
- 10 y. *Regional Chief Information Security Officer (RCISO)* refers to a cybersecurity official
11 designated by the NCSA, in coordination with the Department of Information and
12 Communications Technology (DICT), with specific role created for government
13 agencies, government-owned and controlled corporations (GOCCs), and other covered
14 entities that are unable to create a dedicated *plantilla* position for an Individual CISO.
15 They can also be referred to as Group CISO under this Act.
- 16 z. *Responsible disclosure* refers to the practice of not disclosing the vulnerability until the
17 CII responsible for the hardware or software deals fixes the vulnerability.
- 18 aa. *Sectoral computer emergency response team (SCERT)* refers to a coordinating CERT
19 for CIIS, created for administrative or regulatory agencies that oversee the operations
20 of CII sectors.
- 21 bb. *Security Operations Center (SOC)* refers to the focal point for security operations and
22 computer network defense of an organization. The purpose of the SOC is to defend and
23 monitor an organization's systems and networks on an ongoing basis. The SOC is also
24 responsible for detecting, analyzing, and responding to cybersecurity incidents in a
25 timely manner.

26 CHAPTER II

27 THE NATIONAL CYBERSECURITY AGENCY

28 **SEC. 6. *Creation of the National Cybersecurity Agency.*** – There is hereby created a
29 National Cybersecurity Agency (NCSA), which shall be under the Office of the President.

30 The NCSA is hereby granted the authority to issue baseline operational directives to all
31 government agencies, offices, and instrumentalities, to compel any covered entity to abide by
32 its orders or take action on a matter affecting cybersecurity.

33 Nothing in this Act shall be construed as to diminish or deprive the jurisdiction conferred
34 by law upon other government agencies concerning the powers that they exercise under their

1 respective mandates.

2 **SEC. 7. *Mandate.*** – The NCSA shall be the primary policy, planning, coordinating,
3 implementing, and administrative entity that will plan, develop, coordinate, and implement the
4 overall national cybersecurity strategy of the government.

5 **SEC. 8. *Powers and Functions.*** – The NCSA shall exercise the following powers and
6 functions:

7 a. Policy Planning and Coordination

- 8 1. Formulate policies and recommendations on issues concerning cybersecurity,
9 advise Congress and other government agencies on all aspect of cybersecurity, and
10 propose legislation and amendments thereto;
- 11 2. Formulate and implement the National Cybersecurity Plan;
- 12 3. Ensure the participation of all stakeholders in policy formulation and implementation;
- 13 4. Lead the whole-of-government effort to formulate cybersecurity regulations, in
14 accordance with international standards and best practices;
- 15 5. Set technology neutral national standards on the generation, management and use
16 of cybersecurity products, protocols, and cryptographic primitives: *Provided*, That
17 such standards shall not require exclusive reliance on proprietary or vendor specific
18 systems and shall be developed through appropriate stakeholder consultation and
19 independent review;
- 20 6. Coordinate all cybersecurity activities of the government, in partnership with the
21 private sector and other stakeholders;
- 22 7. Advise the President, Congress, Judiciary, and Constitutional bodies on all
23 cybersecurity-related issues and concerns;
- 24 8. Create the National Vulnerability Disclosure Program. The program shall be the
25 gateway for the security researchers to submit vulnerabilities of the online assets of
26 the Philippine government and provide measures to create a safe environment for
27 security researchers to responsibly disclose cybersecurity incidents;
- 28 9. Establish a multisectoral cooperation framework composed of the private sector,
29 academic institutions, and industry stakeholders to ensure continuity, shared
30 responsibility, and alignment of national cyber resilience efforts, including
31 mechanisms for threat intelligence sharing;
- 32 10. Periodically issue and update guidance on the adoption of current and
33 internationally recognized best practices, technologies, and minimum cybersecurity
34 standards;

11. Adopt a risk-based information protection framework, including the designation of classified information and controlled information, in accordance with standards and procedures to be prescribed in the implementing rules and regulations, consistent with national security requirements and the effective performance of cybersecurity functions;
 12. Advise the DICT on the cybersecurity aspects of ICT asset disposal; and
 13. Publish or issue official directives and administrative issuances, orders, and circulars, which include rules of procedure in the exercise of its mandate and the schedule of administrative fines and penalties for violations of the Act.
- b. CII Protection
1. Formulate and set minimum cybersecurity standards for CIIs, including Operational Technology (OT) security and Industrial Control System (ICS) standards, in coordination with relevant administrative agencies exercising regulatory functions over CIIs;
 2. Ensure compliance of CIIs to cybersecurity minimum standards requirements;
 3. Conduct audit and assessment of the cybersecurity posture of CIIs, all NGAs, including GOCCs, SUCs, and LGUs; *Provided*, That the Armed Forces of the Philippines (AFP) and National Intelligence Coordinating Agency (NICA) shall maintain operational autonomy over their respective systems. The Congress and the Judiciary may request the NCSA to assist them in the conduct of cybersecurity audit and assessment;
 4. Nothing in this Act prevents a government agency or sector regulator from requiring a CII entity under its jurisdiction to implement additional standards, or other standards higher than the minimum set by the DICT, as deemed necessary;
 5. Establish a liaison network of CERTs or CERTs Points of Contact, among CIIs to facilitate communication and information sharing;
 6. Regulate and provide oversight over private cybersecurity service providers such as, but not limited to Vulnerability Assessment and Penetration Testing (VAPT) service providers, and security operations center providers; and
 7. Upon request, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators, and if appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other government departments and agencies; and
 8. Provide technical assistance to the AFP and NICA upon their request to support their

- 1 internal cybersecurity efforts.
- 2 c. Cyber Threats and Incidents Response
- 3 1. Establish the NCERT and a robust incident response capability to promptly detect,
- 4 analyze, and mitigate cybersecurity incidents involving information technology (IT)
- 5 systems, OT, and ICS affecting national security or public interest and to collaborate
- 6 with relevant government agencies, private sector entities, and international partners
- 7 for coordinated incident response;
- 8 2. Enhance cybersecurity threat intelligence and situational awareness through the
- 9 establishment of information-sharing protocols between the NCSA and government
- 10 agencies;
- 11 3. Establish a liaison network of CERTs or CERTs Points of Contact, among
- 12 government agencies to support the implementation of the mandate of NCERT;
- 13 4. Perform vulnerability assessment and penetration testing initiatives on IT, OT, and
- 14 ICS, to detect, identify, and analyze cybersecurity threats and to coordinate with law
- 15 enforcement authorities for the proper attribution of cyber-attacks against CII;
- 16 5. Determine the nature and classification of cyber threats and refer incidents to
- 17 appropriate agency, including, but not limited to the NICA, AFP, Department of
- 18 Justice (DOJ), and the National Privacy Commission (NPC), Philippine National
- 19 Police (PNP), National Bureau of Investigation (NBI) and Cybercrime Investigation
- 20 and Coordinating Center (CICC); and
- 21 6. Collect open-source data strictly for technical threat intelligence, vulnerability
- 22 assessment, and cybersecurity incident prevention or response, excluding content
- 23 regulation, opinion monitoring, or speech analysis, and only insofar as such data is
- 24 necessary to address a material cybersecurity threat.
- 25 d. Research and Development
- 26 1. Lead and support research and development (R&D) efforts focused on new and
- 27 emerging cybersecurity technologies, tools, and standards, in partnership with the
- 28 academe, other government research institutions, and international partners; and
- 29 2. Study and recommend to Congress fiscal and non-fiscal incentives including tax
- 30 credits and grants, to encourage and support private sector research and
- 31 development efforts in cybersecurity technologies and solutions.
- 32 e. Capacity Building
- 33 1. Develop and implement training programs to build and maintain a highly skilled
- 34 cybersecurity workforce in the government, in coordination and cooperation with the

1 ICT Academy of the Philippines;

- 2 2. Develop and execute a partnership framework with academic institutions, industry
3 stakeholders, and foreign counterparts to promote knowledge sharing, resource
4 sharing, and skills development in cybersecurity;
- 5 3. Prescribe personnel qualifications and other qualification standards essential to the
6 effective development on cybersecurity field of expertise;
- 7 4. Co-develop with the Civil Service Commission (CSC) the cybersecurity qualification
8 standards;
- 9 5. Promote the development of cybersecurity courses, programs, and training in
10 partnership with the Commission on Higher Education (CHED), SUCs, and Technical
11 Education and Skills Development Authority (TESDA); and
- 12 6. Develop and establish a public-private partnership (PPP) framework for cybersecurity
13 to leverage private sector expertise, technology and capital for cybersecurity
14 infrastructure development.

15 f. Information Sharing

- 16 1. Establish and maintain a NSOC to gather, assess, and distribute actionable
17 intelligence regarding cyber threats, emerging patterns, and potential vulnerabilities,
18 thereby bolstering the nation's cybersecurity situational awareness and facilitating
19 informed decision-making processes;
- 20 2. Develop a mechanism for voluntary information-sharing between the government (or
21 public) and the private sector;
- 22 3. Issue cybersecurity advisories or guidelines regularly or as needed;
- 23 4. Establish information-sharing protocols between the agency and government
24 agencies on all information relevant to cybersecurity; and
- 25 5. Oversee the development of mechanisms for international threat intelligence
26 exchange.; and
- 27 6. Formulate and establish information sharing protocols between the agency and
28 government agencies on all information relevant to cybersecurity.

29 g. International Cooperation

- 30 1. Foster international collaboration and cooperation for the promotion of cybersecurity
31 including through formal agreements that enhance shared defense, capacity-building,
32 and threat intelligence exchange;
- 33 2. Support the government's efforts to establish the Philippines as a regional digital
34 hub; and

- 1 3. Provide support to the Department of Foreign Affairs (DFA), as the lead for all
2 international representations, on matters concerning international cybersecurity
3 cooperation.
- 4 h. Establish, categorize, and maintain a registry of identified cybersecurity risks and threats
- 5 i. Regulation and Referral
- 6 1. Recommend to the DOJ the prosecution and imposition of penalties specified under
7 Chapter VI of this Act;
- 8 2. Exercise such other powers as may be provided by law, as well as those which may
9 be implied from, or which are necessary or incidental to the carrying out of the express
10 powers granted the NCSA to achieve the objectives and purposes of this law.
11 *Provided, however,* that the regulatory authority of the NCSA shall be ancillary to any
12 duly constituted regulatory jurisdiction granted to any agency by existing laws, such
13 as but not limited to, the NPC, BSP, *et.al.* *Provided further,* that reasonable notice to,
14 and coordination with the appropriate regulatory agency shall be made by the NCSA
15 prior to the enforcement of the provisions of this Act. Unless expressly specified,
16 nothing in this Act shall be constructed as to diminish or deprive the regulatory
17 jurisdiction conferred by law upon other government agencies concerning the service
18 that they regulate;
- 19 3. The NCSA shall have the authority to endorse such matter to the appropriate
20 member-agency or competent authority for proper investigation, enforcement, or
21 prosecution, as may be warranted, upon finding reasonable grounds to believe that
22 additional violations have been committed falling within the jurisdiction of such agency
23 in the course of its investigation. The concerned agency shall take appropriate action
24 in accordance with its mandate, without prejudice to the concurrent powers and
25 proceedings of the NCSA under this Act; and
- 26 4. The NCSA shall perform all other acts as may be necessary to effectively implement
27 the provisions of this Act and to issue orders, resolutions or decisions, including the
28 imposition of administrative sanctions, fines, or penalties, for violations of this Act.
- 29 j. Cybersecurity Certification
- 30 1. The NCSA shall promulgate rules and procedures for certifying cybersecurity
31 trustworthiness of service, suppliers, or technologies. Towards this end, the NCSA in
32 consultation with other government agencies and the private sector shall devise a
33 rating or scoring system for assessing information security and cybersecurity
34 standards considering various criteria. Such scoring system shall be reviewed

periodically at least once every two (2) years or as may be deemed necessary by the NCSA. The NCSA may charge reasonable fees to defray the administrative cost of the services rendered, subject to existing laws and regulations; and

2. The certification issued by NCSA shall be valid for a maximum period of two (2) years; *Provided*, that NCSA, may impose a shorter validity period depending on the criticality of the business or the cybersecurity risks relevant to the business of the person; and *Provided further*, that the NCSA, upon recommendation by NCERT, may require re-certification prior to the expiration of the certification due to factors increasing the cybersecurity risks relevant to the business of the person.

SEC. 9. Composition. – The NCSA shall be headed by a Director General with the rank of Secretary and shall be assisted by two (2) Deputy Directors-General with the rank of Undersecretary and three (3) Assistant Directors-General with the rank of Assistant Secretary.

SEC. 10. Term of Office. – The term of office of the Director General, the Deputy Directors-General, and the Assistant Directors-General shall be three (3) years, subject to reappointment by the President of the Philippines. In case a vacancy occurs before the expiration of the term of office, the appointment to such vacancy shall only be for the unexpired term of the predecessor.

SEC. 11. Qualifications. – The following are the minimum qualifications of the Director-General and Deputy Directors-General of the NCSA:

- a. *Director-General* – The Director-General shall be appointed by the President. No individual shall be appointed as Director-General of the NCSA unless such person is a Filipino citizen domiciled in the Philippines, of good moral character, has at least five (5) years of government experience and ten (10) years cumulative experience as a cybersecurity, information privacy, or information security professional, and has at least a Master's Degree in Cybersecurity, Information Security, or any other related master's degree.
- b. *Deputy Directors-General* – The Deputy Directors-General of the NCSA shall be appointed by the President. No individual shall be appointed Deputy Directors-General of the NCSA unless such person is a Filipino citizens domiciled in the Philippines, of good moral character, possessing proven integrity, and unquestionable integrity, with a track record of leadership, recognized competence with the appropriate educational background in cybersecurity or any related field, with at least six (6) years of supervisory or management experience in the field of cybersecurity, data privacy, information technology (IT), IT risk management, or any combination thereof.

SEC. 12. Separation and Retirement from Service. – Affected officials and personnel who will not be transferred to or absorbed under the NCSA may avail of the applicable retirement or separation benefits under the existing retirement or separation laws, as the case may be.

SEC. 13. Organizational Structure and Staffing Pattern. – The NCSA shall determine its organizational structure and staffing pattern subject to the evaluation and approval of the Department of Budget and Management (DBM), in accordance with the civil service and other pertinent laws, rules, and regulations.

SEC. 14. Transfer of Agencies and Personnel to the NCSA. – The Department of Information and Communications Technology-Cybersecurity Bureau (DICT-CSB) and its corresponding Divisions along with their powers and functions, applicable funds and appropriations, records, equipment, property, and personnel, are hereby transferred to the NCSA.

All offices, services, divisions, units, and personnel not otherwise covered by this Act for transfer to NCSA, shall be retained under the DICT which shall continue to operate under its current name and functions.

The NCSA shall be under the Office of the President for policy and program coordination, and shall continue to operate and function laterally and in accordance with prevailing laws:

- a. All powers and functions related to cybersecurity, including but not limited to the formulation of the National Cybersecurity Plan, establishment of the NCERT, and the facilitation of international cooperation on intelligence regarding cybersecurity matters, are hereby transferred to NCSA;
- b. The laws and rules on government reorganization as provided for in Republic Act No. 6656, otherwise known as the Reorganization Law, shall govern the reorganization process of NCSA; and
- c. The transfer of functions, assets, funds, equipment, properties, transactions, and personnel of the affected agencies to NCSA shall be completed within six (6) months from the effectivity of this Act. During this transition period, existing personnel shall continue to assume their posts in holdover capacities until new appointments are issued. After the transfer of the agencies specified in this section, the NCSA, in coordination with DBM, shall determine and create new positions, the funding requirements of which shall not exceed twenty-five percent (25%) of the equivalent cost of positions abolished.

SEC.15. Relationship of NCSA with Other Cyber Entities. – Consistent with the whole-of-government approach, the NSCA will ensure alignment of efforts and priorities by maintaining close coordination with agencies with mandates related to national security, cybersecurity, and

1 cybercrime.

- 2 a. The NCERT, which is within the authority of the NSCA, shall work within a strict chain of
3 command with all other CERTs. It shall also coordinate their efforts with the Defense-
4 cert as the national coordinating CERTs.
- 5 b. The NSCA, through the NSOC, shall send data and threat information to the National
6 Cybersecurity Intelligence Network (NCIN), a cyber fusion center operated by the NICA,
7 so that it can process and provide actionable intelligence and important situational
8 awareness to both the NCERT and the Defense-cert.
- 9 c. The NCSA, upon determination that a series of cybersecurity incidents are attributable
10 to a state-sponsored threat actor, shall hand over the response activities to the Defense-
11 cert.
- 12 d. The NCSA, upon determination that a cybercrime is present in an incident they are
13 responding to, shall escalate the matter for proper turn-over to The Philippine National
14 Police Anti-Cybercrime Group or the National Bureau of Investigation -Cybercrime
15 Division.

16 CHAPTER III

17 CRITICAL INFORMATION INFRASTRUCTURE

18 **SEC. 16. *Designation of Critical Information Infrastructure (CII)*.** – The NCSA will
19 have the duty and power to oversee the CIIs in the Philippines.

- 20 a. The NCSA shall identify entities that own, operate or maintain CII using a risk-based
21 approach, as prescribed by the NCSP and shall adopt a set of criteria for identifying CIIs.
- 22 b. After the confirmation of the CII designation, the NCSA shall issue a written notice to the
23 owner of the computer or computer system, designating said system as a CII for the
24 purposes of this Act.
- 25 c. A notice issued under subparagraph (a) shall:
 - 26 1. Identify the computer or computer system that is being designated as a CII;
 - 27 2. Identify the owner of the computer or computer system so designated as a CII;
28 Inform the owner of the computer or computer system, regarding the owner's duties
29 and responsibilities under this Act that arise from the designation;
 - 30 3. Inform the owner of the computer or computer system that any representation against,
31 or a decision on the designation, may be challenged and to provide information on
32 the applicable procedure.
- 33 d. Any designation under subparagraph (a) shall be in effect for a period of five (5) years,
34 unless it is withdrawn by the NCSA before the expiration of the period.

1 **SEC. 17. Regulation of Providers of Essential Services Who Rely on Third-party**

2 **Owned CII.** – Providers remain responsible for the cybersecurity and resilience of the computer
3 systems they rely on to deliver essential services, even if those systems are managed by a third
4 party. Providers who depend on third-party-owned CII shall secure legally binding commitments
5 from these vendors ensuring that the third party meets the cybersecurity standards and
6 requirements applicable to CII, including incident reporting, auditing, and risk assessment.

7 **SEC. 18. Compliance Requirements for Organizations and the CII.** – The NCSA

8 shall, in coordination with concerned government regulatory agencies, create a list of compliance
9 requirements for CII. In determining the compliance requirements for organizations and CII,
10 due consideration shall be given to minimizing their impact on the cost of services provided by
11 the organizations and CII. These shall include the following:

- 12 a. List of authorized personnel and their level of access to the computer system labeled
13 as CII;
- 14 b. The cybersecurity or information security framework used for risk assessment and
15 adoption of technical and procedural controls;
- 16 c. Initial audit report;
- 17 d. Cybersecurity incident handling organization and protocol being implemented by the
18 CII operator;
- 19 e. Organization and technical contact persons of the CII operators;
- 20 f. The OT or ICS utilized, when applicable; and
- 21 g. Such other information, as may be required by the NCSA.

22 **SEC. 19. Cybersecurity Audit and Risk Assessment of CII.** – All CII operators shall

23 take the necessary steps to identify, assess, and institute technical or procedural controls to
24 mitigate cybersecurity risks related to the CII at least once every three (3) years.

25 At least once every two (2) years (or at such higher frequency as may be directed by the
26 NCSA in any particular case), all CII operators must submit an authenticated cybersecurity audit
27 and risk assessment report performed by a NCSA recognized auditing firm that specializes in
28 cybersecurity. Cybersecurity audit and risk assessment reports shall be submitted to NCSA and
29 shall be kept in record for a period of not less than five (5) years.

30 To complement the authenticated cybersecurity audit and risk assessment report, all cii
31 operators shall implement continuous monitoring, asset management and vulnerability
32 management processes to identify and mitigate cybersecurity risks affecting critical systems.

33 **SEC. 20. Mandatory Disclosure of Cybersecurity Incidents on CII.** –

- 34 a. Organizations operating CII shall notify their government regulator and NCSA,

- 1 through the NCERT, upon discovery of a critical or high-risk cybersecurity incident;
- 2 b. NCSA shall define the taxonomy, including classification and categorization of which
- 3 cybersecurity incidents are considered “critical”, “high risk” and “moderate”. For
- 4 moderate risk cybersecurity incidents, the CII operator shall inform NCSA or NCERT
- 5 of the incident; for data breaches, whereby the affected agency to the NPC;
- 6 c. In the event of attacks restricting access to ICT and data, the affected CII entities are
- 7 required to disclose in their report whether they have made any payments or complied
- 8 with the demands of the threat actor; and
- 9 d. CERTs shall coordinate with law enforcement authorities in the filing of cybercrime
- 10 cases.

11 **SEC. 21. Assistance Extended by the Government to CII Operators.** – Operators of

12 CII may request assistance for NCSA to provide the following:

- 13 a. Use of government technical controls and systems for the defense and protection of
- 14 the CII;
- 15 b. Priority co-location with government data centers subject to availability;
- 16 c. Use of government secure crypto-primitives such as but not limited to, digital certificates;
- 17 and
- 18 d. Knowledge management platform to facilitate faster sharing of information between
- 19 the industry, NCSA, government regulators, and other concerned organizations.

20 **SEC. 22. Confidentiality of CII Related Documents.** – The official list of CIIs, including

21 the assessment, evaluation, audit, and technical reports shall be considered documents related

22 to National Security and thus, are considered confidential and classified. The proper authority

23 by law, administrative or legal order, and upon the recommendation of NCSA, may declassify

24 these documents.

25 If a subpoena duces tecum is issued for any of these classified documents, NCSA shall

26 inform the body who ordered the subpoena that the document can only be opened or scrutinized

27 in an executive session and shall be disclosed only to a limited number of people on a strict

28 need-to-know basis.

29 **SEC. 23. Withdrawal or Removal of CII Designation.** – The NCSA, through a written

30 resolution, may withdraw or remove the designation of any CII at any time if the NCSA is of the

31 opinion that the computer or computer system no longer fulfills the criteria of a CII. The NCSA

32 shall notify in writing the CII operator of the withdrawal or removal of such designation within

33 fourteen (14) days from the issuance of the resolution.

34 CHAPTER IV

CYBERSECURITY REQUIREMENTS

SEC. 24. Adoption of Minimum Cybersecurity Requirements (ASC). – All national government agencies, government instrumentalities, government-owned or -controlled corporations, and local government units shall adopt and implement, in consultation with relevant government agencies, sector regulators, and stakeholders, minimum cybersecurity and resilience measures to protect information systems, networks, and digital services against cybersecurity threats and disruptions.

Such measures shall be risk-based, proportionate, and aligned with internationally recognized cybersecurity and information security standards, as may be prescribed and regularly updated by the NCSA.

For purposes of statutory neutrality and international interoperability:

- a. The baseline requirements shall be anchored on internationally recognized standards, including, but not limited to, ISO/IEC information security and resilience standards, or their functional equivalents;
- b. Detailed technical controls, sector-specific frameworks, and implementation guidance may be adopted through implementing rules, regulations, or sectoral issuances, consistent with evolving global best practices;
- c. Compliance obligations shall remain proportionate to the risk profile, scale, and criticality of the covered entity; and
- d. Nothing in this Act prevents a government agency or sector regulator for implementing additional standards, or other standards higher than the minimum set by the NCSA, as deemed necessary.

SEC. 25. Creation of a Chief Information Security Officer (CISO). – Pursuant to this Act, a CISO *plantilla* position shall be created or designated for all covered entities who will:

- a. Establish, implement, and maintain the organization's information security program;
- b. Develop program guidelines for continuous monitoring;
- c. Consolidate and analyze organizational security weaknesses and deficiencies;
- d. Acquire or develop and maintain tools to support information security;
- e. Provide training on the organization's security program and processes; and
- f. Provide support to information owners and information system owners on how to implement security for their information systems.

The CISO shall lead the GCERT and shall serve as the primary liaison to the agency's authorizing officials, information system owners, information system security officers, and the SCERT and the NCERT. Creation of CISO shall be subject to the review and evaluation of the

1 DBM and CSC.

2 *Provided*, that for government agencies, GOCCS, and other entities covered by law
3 unable to create a position for CISO, the NCSA, in coordination with DICT, shall designate
4 regional or group CISO, as mandated by this Act.

5 The CISO ensures that information resources and technologies are effectively
6 protected. CISOs oversee the development, implementation, and enforcement of security
7 policies. The CISO might also work alongside the chief information officer in procuring
8 cybersecurity products and services, and managing disaster recovery and business continuity
9 plans.

10 CHAPTER V

11 PROHIBITED ACTS AND PENALTIES

12 **SEC. 26. *Unauthorized Disclosure of CII Confidential Information.*** – Any individual
13 who discloses CII-related documents and information without right, in accordance with Sections
14 22 and 35, shall be held liable under this Act.

15 **SEC. 27. *Non-compliance of CII Operators.*** – In the event that a CII operator fails
16 willfully or negligently to comply with the orders, directive, mandate, remediation, and any other
17 regulations of NCSA, the same shall incur penalties as provided for this Act. This includes
18 submission of documentary requirements, and providing NCSA access to necessary computer
19 data during investigations of cyber-attacks.

20 **SEC. 28. *Penalties.*** – The following penalties shall be applied for violations of this Act:

21 a. *Unauthorized Disclosure of CII Confidential Information.* – any person who discloses,
22 transmits, alters, or makes accessible cybersecurity-sensitive information obtained
23 by reason of their functions, duties, or access in relation to CII systems, networks,
24 or operations, without lawful authority, shall be punished by imprisonment of six (6)
25 years and one (1) day to twelve (12) years, or a fine of not less than Two million
26 pesos (₱2,000,000.00), or both.

27 b. *Administrative Liability of CII Operators.* – upon determination of a violation of this
28 Act, its implementing rules and regulations, or other relevant issuances, the NCSA
29 may impose the following:

30 1. A fine of at least Five thousand pesos (Php 5,000.00) but not exceeding Two
31 million pesos (Php 2,000,000.00) per violation: *Provided*, that if the CII operator
32 has a gross annual income not exceeding Ten million pesos (Php 10,000,000.00),
33 the imposable penalty shall be equivalent to one percent (1%) to two percent
34 (2%) of its gross annual income; and

2. A fine of at least Three hundred thousand pesos (Php 300,000.00) but not exceeding Five million pesos (Php 5,000,000.00): *Provided*, that if the CII operator has a gross annual income of Ten million pesos and above (Php 10,000,000.00), the imposable penalty shall be equivalent to one percent (1%) to two percent (2%) of its gross annual income;

The administrative fines imposed under this Act shall be adjusted by the NCSA annually, considering the prevailing cost of money based on the current consumer price index, and subject to the publication of such adjustments.

SEC. 29. *Liability Under Other Laws.* – A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

CHAPTER VII

FINAL PROVISIONS

SEC. 30. *Authority to Accept Assistance and Donations.* – The NCSA is authorized to accept donations, contributions, grants, bequests or gifts from domestic or foreign sources, for purposes relevant to its mandates and functions, subject to existing laws, rules and regulations.

SEC. 31. *Appropriations.* –The amount necessary for the initial implementation of this Act shall be charged against the current year's appropriations of the DICT. Thereafter, such amounts as may be necessary for the continued implementation of this Act shall be included in the Annual General Appropriations Act.

SEC. 32. *Joint Congressional Oversight Committee on Cybersecurity and CIIP.* - There shall be created a Joint Congressional Oversight Committee on Cybersecurity and CIIP (JCOCCC) which shall monitor and ensure the effective implementation of this Act. It shall determine weaknesses and loopholes in the law, recommend the necessary remedial legislation or administrative measures and perform such other duties and functions as may be necessary to attain the objectives of this Act.

The JCOCCC shall be composed of four (4) members from the Senate and four (4) members from the House of Representatives, in addition to the Chairperson of the Senate Committee on Science and Technology and the Chairperson of the House of Representatives Committee on Information and Communications Technology: *Provided*, That one (1) member from each chamber shall come from the minority party/bloc.

The Chairperson of the Senate Committee on Science and Technology and the Chairperson of the House of Representatives Committee on Information and Communications Technology shall act as co-Chairpersons of the JCOCCC. The Secretariat of the JCOCCC shall

1 come from the existing Secretariat personnel of the Committee on Science and Technology of
2 the Senate and the Committee on Information and Communications Technology of the House of
3 Representatives.

4 The JCOCCC shall exist for a period not exceeding five (5) years from the effectivity of this
5 Act. Thereafter, its oversight functions shall be exercised by the Senate Committee on Science
6 and Technology and the House of Representatives Committee on Information and
7 Communications Technology, acting separately.

8 **SEC. 33. Report.** – The NCSA shall submit an annual report to the Office of the President
9 on the implementation of this Act, as well as the operations of the NCSA. The NCSA shall also
10 include in its report disclosures of cybersecurity vulnerabilities, actionable protocols to mitigate
11 cybersecurity vulnerabilities to information systems and industrial control systems. The NCSA
12 shall likewise publish a “State of Cybersecurity in the Philippines” report for covered entities and
13 the general public.

14 **SEC. 34. Confidentiality.** –

- 15 a. All parties involved in the application of this Act shall respect the confidentiality of
16 information and data obtained in carrying out their tasks and activities in such a
17 manner as to protect, in particular:
- 18 1. Intellectual property rights, and confidential business information or trade secrets
19 of a natural or juridical person, including source code, except in cases where the
20 disclosure and access is necessary to protect the legitimate interest recognized
21 by existing laws, rules, and regulations;
 - 22 2. Public and national security interests;
 - 23 3. Data of security agencies, ensuring that they will not be migrated into the private
24 domain; and
 - 25 4. Integrity of criminal or administrative proceedings.
- 26 b. Without prejudice to paragraph (a), information exchanged on a confidential basis
27 between government departments, agencies, bureaus, offices, and institutions and
28 the NCSA shall not be disclosed without the prior agreement of the originating
29 government departments, agencies, bureaus, offices, and institutions.
- 30 c. Adequate protection shall be set in place between the information shared by the
31 private sector and government agencies, particularly security and law enforcement
32 agencies.
- 33 d. Paragraphs (a) and (b) shall not affect the rights and obligations of the NCSA and
34 notified bodies with regard to the exchange of information and the dissemination of

warnings, nor the obligations of the persons concerned to provide information under existing laws, rules, and regulations.

- e. The NCSA may exchange, when necessary, sensitive information with relevant authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of protection.

SEC. 35. *Periodic Review.* – The NCSA, in consultation with the DICT, the DOST, and other concerned agencies shall conduct a review of the Act every three years, or more frequently as may be necessary, to ensure that certifications, regulations, standards, penalties, and other provisions of the Act, with the end in view of meeting the cybersecurity standards and requirements for emerging technologies.

SEC. 36. *Fees, Fines, and Penalties.* – All fees, fines, and penalties collected by the NCSA pursuant to this Act shall be collected and deposited with the National Treasury as income of the general fund.

SEC. 37. *Implementing Rules and Regulations (IRR).* – Within one hundred twenty (120) days after the effectivity of this Act, the DICT, the DBM, the CSC, and upon consultation with relevant stakeholders, shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 38. *Transitory Provisions.* – For purposes of administrative efficiency and to prevent the duplication of functions, the powers, functions, duties, and responsibilities of the Cybersecurity Bureau of the DICT are hereby transferred to and absorbed by the NCSA.

The NCSA shall establish a phased implementation schedule in the IRR, prioritizing the most critical sectors and highest-risk entities. Entities that hold international certifications at the time of effectivity of this Act shall be deemed to be in compliance during the transitory period.

All new positions created under this Act shall be prioritized, subject to the review and approval of the DBM consistent with civil service laws, rules and regulations. Moreover, until such time that the government shall have completed the transition in accordance with the objectives of this Act, all government activities covered under this Act shall be conducted in the manner provided under existing laws and rules.

The government shall complete the transition within a period of two (2) years from the effectivity of this Act.

SEC. 39. *Separability Clause.* – If any provision of this Act is declared invalid or unconstitutional, the remainder thereof not otherwise affected shall remain in full force and effect.

SEC. 40. *Repealing Clause.* – All laws, presidential decrees, executive orders, letters of instructions, proclamations, or administrative regulations that are inconsistent with the provisions

1 of this Act are hereby repealed, amended, or modified accordingly.

2 **SEC. 41. *Effectivity*.** – This Act shall take effect fifteen (15) days after publication in the
3 *Official Gazette* or in a newspaper of general circulation.

4 *Approved,*

FACT SHEET

House Bill No. 9605

(In Substitution of House Bills Numbered 9, 620, 660, 919, 1922, 2193, 2826, 3193, 3822, 4187, 4191, 4381, 5154, 5487, 5592, 6090, 6485, 6768, 6818, 7202, 7203, 7359, 7927, 8071, 8096, 8482, 8707, and 9197)

NATIONAL CYBERSECURITY AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 2026

Introduced by: REPRESENTATIVES MIGUEL LUIS R. VILLAFUERTE, VINCENZO RENATO LUIGI R. VILLAFUERTE, TSUYOSHI ANTHONY "HORI" G. HORIBATA, TERRY L. RIDON, FERDINAND MARTIN G. ROMUALDEZ, ANDREW JULIAN K. ROMUALDEZ, JUDE A. ACIDRE, JURDIN JESUS M. ROMUALDO, KEITH MICAH "ATTY. MIKE" D.L. TAN, BERNADETTE S. BARBERS, ATTY. GERVILLE "JINKY BITRICS" R. LUISTRO, BRIAN POE, EMILIO BERNARDINO L. YULO, JAVIER MIGUEL LOPEZ BENITEZ, BRYAN B. REVILLA, LANI MERCADO-REVILLA, RAMON JOLO B. REVILLA III, YEDDA MARIE K. ROMUALDEZ, JUAN CARLOS "ARJO" C. ATAYDE, SALVADOR A. PLEYTO, AUDREY KAY T. ZUBIRI, EDVIC G. YAP, ERIC GO YAP, ERIC L. OLIVAREZ, ALFRED C. DELOS SANTOS, ALEXANDER TY PIMENTEL, BRIAN RAYMUND S. YAMSUAN, CHRISTOPHERSON "COCO" M. YAP, JAIME R. FRESNEDI, MA. NINA FRANCESCA P. LACSON, RICARDO JR. S. CRUZ, JOCELYN P. TULFO, RALPH WENDEL P. TULFO, MIKAELA ANGELA B. SUANSING, NATHANIEL M. ODUCAO, KRISTINE SINGSON-MEEHAN, RONALDO V. PUNO, YEYGENY VINCENTE B. EMANO, MARIA RACHEL J. ARENAS, ALFREDO "ALBEE" B. BENITEZ, JULIUS CESAR "JAY" V. VERGARA PATRICK MICHAEL D. VARGAS, ALYSSA MICHAELA "MICA" M. GONZALES, BERNADETTE G. ESCUDERO, ANNA VICTORIA VELOSO-TUAZON, EDUARDO R. RAMA JR., ANTONIO L. TINIO, AGATHA PAULA AGUILAR CRUZ, JOSE MANUEL TADEO "CHEL" I. DIOKNO, MARIA CRISTINA C. ANGELES, ANTONIO "TONYPET" T. ALBANO, MILAGROS AQUINO-MAGSAYSAY, KAREN HOPE F. GARCIA, ANTONINO B. ROMAN III, STEVE CHIONGBIAN SOLON, LEODY "ODIE" F. TARRIELA, NOEL "BONG" N. RIVERA, JAMES "JOJO" ANG JR., ZIAUR-RAHMAN "ZIA" ALONTO ADIONG, ANTOLIN A. ORETA III, CLAUDINE DIANA D. BAUTISTA-LIM, CHARISSE ANNE C. HERNANDEZ, RUTH M. SAKALURAN, IRIS MARIE DEMESA MONTES, REYNANTE U. ARROGANCIA, GERARDO "GERRYBOY" J. ESPINA JR., JOHN TRACY F. CAGAS, FAUSTINO MICHAEL CARLOS T. DY III, FERDINAND "B1" L. BELTRAN, MARIA KRISTINA JIHAN B. GLEPA, MA. VICTORIA CO-PILAR, CHEENO MIGUEL D. ALMARIO, JESUS "JESS" R. MARQUEZ, MARIA ANGELA S. GARCIA, EMMANUEL L. IWAY, RICHELLE SINGSON, REBECCA MARIA ALCANTARA YNARES, JOSE MANUEL "JM" F. LAGDAMEO, ADRIAN E. SALCEDA, JAN "ATTY. JP" DL. PADIERNOS, ANGELO MARCOS BARBA, DADAH KIRAM ISMULA, ROMAN T. ROMULO, EULOGIO "LEO" R. RODRIGUEZ, EDGAR R. ERICE, TOBIAS "TOBY" M. TIANGCO, ROBERT NAZAL, JANETTE L. GARIN, JOSE "BONG" J. TEVES, JR., ALBERT S. GARCIA, JOSE C. ALVAREZ, LORETO S. AMANTE, ARNIE B. FUENTEBELLA, DANTE S. GARCIA, ALEXANDRIA "QUEENIE" GONZALES, MONIQUE YAZMIN MARIA Q. LAGDAMEO, MA. CHRISTINA TALAVERA LOPEZ, ROMEO S. MOMO SR., RUFUS B. RODRIGUEZ, MA. ISABEL L.

SAGARBARRIA, JOSEPH S. TAN, AMADO CARLOS A. BOLILIA IV, PATRICIA C. CALDERON, TIMOTHY JOSEPH E. CAYTON, MAXIMO Y. DALOG JR., FELIMON M. ESPARES, NELSON S. LEGACION, CARLOS ANDES LORIA, DIBU S. TUAN, ROLANDO M. VALERIANO, FLORABEL C. YATCO, ARLYN P. AYON, ELIJAH RUMBAOA SAN FERNANDO, JAN FRANZ NORBERT JOSELITO A. CHAN, GERALD CLOYD ALEXIS V. GALANG, ATTY. JENNIFER “KAREN” A. LAGBAS AND LINABELLE RUTH R. VILLARICA.

Committee Referral: **COMMITTEE ON INFORMATION AND COMMUNICATIONS TECHNOLOGY**

Committee Chairperson: **Hon. MIGUEL LUIS R. VILLAFUERTE**

OBJECTIVES:

- To ensure a safe, reliable, and resilient digital environment that protects national security and prevents threats to government operations;
- To protect individuals and organizations from cyber threats such as fraud, identity theft, data breaches, ransomware and other malicious activities; and
- To safeguard public safety and welfare from harmful effects of disruptions to essential services.

KEY PROVISIONS:

- Establishes and implements cybersecurity standards and certification systems for organizations, service providers, technologies, and cybersecurity professionals to ensure consistent, high-quality security practices across sectors.
- Cultivates a highly skilled cybersecurity workforce by developing specialized training programs, qualification standards, and strong partnerships with academia, industry, and international partners.
- Mandates the establishment of the National Cybersecurity Agency (NCSA) under the Office of the President as the primary body responsible for national cybersecurity policy, planning, coordination, and implementation.
- Enumerates the powers and functions of NCSA which include the following:
 - a. **Policy Planning and Coordination** – Formulates national cybersecurity policies and standards, coordinates stakeholders, advises decision-makers, and issues directives shaping national cybersecurity strategy;
 - b. **CII Protection** – Sets standards, audits compliance, regulates cybersecurity providers, and provides technical support to high-risk sectors;
 - c. **Cyber Threats and Incidents Response** – Detects, analyzes, and responds to cyber incidents through the NCERT, coordinated CERT networks, threat

classification, and collaboration with law enforcement and intelligence agencies;

- d. **Research and Development** – Leads cybersecurity R&D and recommends incentives for innovation;
 - e. **Capacity Building** – Develops training, qualification standards, and partnerships to strengthen the cybersecurity workforce;
 - f. **Information Sharing** – Operates the National Security Operations Center and enables timely advisories, information exchange, and intelligence sharing;
 - g. **International Cooperation** – Strengthens global partnerships and supports international cybersecurity collaboration;
 - h. **Cyber Risk Registry** – Maintains a national registry of cybersecurity risks and threats;
 - i. **Regulation and Referral** – Enforces the Act, issue sanctions, recommends prosecutions, and coordinates with sector regulators; and
 - j. **Cybersecurity Certification** – Certifies cybersecurity trustworthiness of services, technologies, and providers through a scoring system and periodic reviews.
- Develops a coordinated national governance framework for cyber resilience that enables proactive, timely, and effective responses to cybersecurity threats and crimes through strengthened detection, investigation, prosecution, and international cooperation.
 - Mandates the NCSA be headed by a Director General with the rank of Secretary, supported by Deputy Directors-General and Assistant Directors-General to ensure effective leadership, coordination, and operational oversight
 - Directs the transfer of the Department of Information and Communications Technology (DICT) Cybersecurity Bureau, including its divisions, functions, assets, and personnel, to the NCSA within six months from the effectivity of the Act, subject to the Reorganization Law, with DICT retaining non-cybersecurity functions.
 - Authorizes the NCSA to identify and designate entities as CIIIs using a risk-based approach, with each designation effective for five years unless withdrawn earlier.
 - Requires CII operators to perform regular audits, risk assessments, and continuous monitoring; submit authenticated reports at least every two years; maintain records for at least five years; report critical and high-risk incidents to the NCSA via NCERT; report moderate incidents to the NCSA or NCERT; report data breaches to the National Privacy Commission; disclose ransom payments; and coordinate with law enforcement on cybercrime cases.

- Protects the critical information infrastructure (CII) by setting and enforcing robust security standards, conducting regular audits and risk assessments, ensuring timely incident reporting, and safeguarding sensitive information essential to national security and critical services.
- Enhances national incident response and threat intelligence capabilities through the National Computer Emergency Response Team (NCERT) and strengthened information-sharing mechanisms.
- Compels government agencies and covered entities to adopt proportionate, risk-based minimum cybersecurity measures aligned with international standards (i.e., ISO/IEC).
- Authorizes the NCSA to issue baseline operational directives, provide technical assistance, and coordinate with the private sector while respecting the autonomy of existing regulators.
- Requires the NCSA to work closely with agencies such as the National Intelligence Coordinating Agency, law enforcement bodies like the Philippine National Police Anti Cybercrime Group and the National Bureau of Investigation Cybercrime Division while recognizing that the Armed Forces of the Philippines maintains operational autonomy over its systems and that other agencies continue to exercise their respective mandates and independent authorities.
- Mandates each National Government Agency, Government-Owned or Controlled Corporation, and Local Government Unit to create or designate a Chief Information Security Officer (CISO) to lead their Government Computer Emergency Response Team (GCERT), oversee the organization's cybersecurity program and information resource protection, and serve as the primary liaison with the NCERT, SCERT, and other relevant stakeholders. For agencies unable to create a dedicated CISO position, allows the designation of a Regional or Group CISO (RCISO) by the NCSA, in coordination with the DICT, to fulfill these responsibilities.
- Imposes the penalties of imprisonment of 6 years and 1 day to 12 years or fines of at least ₱2,000,000 for unauthorized disclosure of CII information, and administrative fines from ₱5,000 to ₱2,000,000 per violation (or 1%–2% of gross annual income for smaller operators), subject to annual adjustment and without prejudice to other applicable laws.
- Creates the Cybersecurity Risk Management and Mitigation Fund, a special fund under the Office of the President sourced from donations, fees, fines, grants, loans, or public-private partnerships, to support NCSA implementation.
- Creates a Joint Congressional Oversight Committee on Cybersecurity and CIIP for a five-year period, after which oversight reverts to the designated Senate and House committees.

- Requires the NCSA to submit an annual report to the Office of the President and publish a public “State of Cybersecurity in the Philippines” report.
- Imposes confidentiality obligations on all parties handling information under the Act, protecting intellectual property, national security, security-agency data, and the integrity of proceedings, while requiring consent for disclosure of inter-agency information and allowing information sharing with foreign partners under confidentiality arrangements.
- Authorizes the NCSA to use collected fees, fines, and penalties for cybersecurity programs, capacity building, research and development, and technology acquisition, while prohibiting use for salaries or personnel benefits and requiring full compliance with government accounting and audit rules.
- Grants the NCSA quasi-judicial authority to issue orders, resolutions, and decisions, including administrative sanctions, fines, and penalties.
- Requires the DICT, Department of Budget and Management, and Civil Service Commission, in consultation with stakeholders, to issue Implementing Rules and Regulations within 120 days.
- Provides a two-year transition period, recognizes existing certifications as compliant during transition, and allows activities to continue under existing rules until full implementation.

RELATED LAWS:

- Executive Orders No. 95 (2019) reorganizing the National Cybersecurity Inter-Agency Committee (NCIAC)
- Republic Act No. 11479 or the Anti-Terrorism Act of 2020
- Republic Act No. 10844 or the Department of Information and Communications Technology Act of 2015
- Republic Act No. 10175 or the Cybercrime Prevention Act of 2012
- Republic Act No. 10173 or the Data Privacy Act of 2012
- Republic Act No. 8439 or the Magna Carta for Scientists, Engineers, Researchers and Other Science & Technology Personnel in the Government
- Republic Act No. 6656 or the Reorganization Law