



HOUSE OF REPRESENTATIVES

H. No. 9605

BY REPRESENTATIVES VILLAFUERTE (M.L.), VILLAFUERTE (V.R.L.), HORIBATA, RIDON, ROMUALDEZ (F.M.), ROMUALDEZ (A.J.), ACIDRE, ROMUALDO, TAN (K.M.), BARBERS, LUISTRO, POE, YULO, BENITEZ (J.M.), REVILLA (B.), MERCADO-REVILLA, REVILLA (R.J.), ROMUALDEZ (Y.M.), ATAYDE, PLEYTO, ZUBIRI, YAP (EDVIC), YAP (ERIC), OLIVAREZ, DELOS SANTOS, PIMENTEL, YAMSUAN, YAP (C.), FRESNEDI, LACSON, CRUZ (R.), TULFO (J.), TULFO (R.W.), DY (F.), MARCOS, SUANSING (M.A.), ODOCADO, SINGSON-MEEHAN, PUNO, EMANO, ARENAS, BENITEZ (A.), VERGARA, VARGAS, GONZALES (A.M.), ESCUDERO, VELOSO-TUAZON, RAMA, TINIO, CRUZ (A.), DIOKNO, ANGELES, ALBANO, AQUINO-MAGSAYSAY, GARCIA (K.H.), ROMAN, SOLON, TARRIELA, RIVERA, ANG, ADIONG, ORETA, BAUTISTA-LIM, HERNANDEZ (C.A.), SAKALURAN, MONTES, ARROGANCIA, ESPINA, CAGAS, DY (F.M.C.), BELTRAN, GLEPA, CO-PILAR, ALMARIO (C.M.), MARQUEZ, GARCIA (M.A.), IWAY, SINGSON (R.), YNARES, LAGDAMEO (J.M.), SALCEDA, PADIERNOS, BARBA, ISMULA, ROMULO, RODRIGUEZ (E.), ERICE, TIANGCO, NAZAL, GARIN, TEVES, GARCIA (A.), ALVAREZ (J.), AMANTE, FUENTEBELLA, GARCIA (D.), GONZALES (A.), LAGDAMEO (M.Y.M.), LOPEZ, MOMO, RODRIGUEZ (R.), SAGARBARRIA, TAN (J.), BOLILIA, CALDERON, CAYTON, DALOG, ESPARES, LEGACION, LORIA, TUAN, VALERIANO, YATCO, AYON, SAN FERNANDO, CHAN (J.F.N.J.), GALANG, LAGBAS, VILLARICA, CARI AND TAN (R.M.)

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), and 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

1 (e) Cybersecurity matters with cross-border or transnational dimensions affecting Philippine
2 interests.

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

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

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

12 (a) *Computer emergency response team (CERT)* refers to a specialized unit responsible
13 for providing services and support for the prevention, detection, handling, and
14 coordination of the response and recovery from computer security incidents like
15 malware infections, cyberattacks, and data breaches.

16 (b) *Computer system* refers to any device or group of interconnected or related devices,
17 one or more of which, pursuant to a program, performs automated processing of data. It
18 covers any type of device with data processing capabilities including, but not limited to,
19 computers and mobile phones. The device consisting of hardware and software may
20 include input, output, and storage components which may stand alone or be connected
21 in a network or other similar devices. It also includes computer data storage devices or
22 media, both physical and virtual.

23 (c) *Confidentiality* refers to property that information is not made available or disclosed to
24 unauthorized individuals, entities, or processes.

25 (d) *Critical information infrastructure (CII)* refers to the computer systems or networks,
26 whether physical or virtual, and/or the computer programs, computer data, and/or traffic
27 data that are vital to this country that the incapacity, destruction, or interference with
28 such systems and assets would have a debilitating impact on security, national or
29 economic security, national health and safety, or any combination of those matter.

30 (e) *Critical infrastructure (CI)* refers to any public service that owns, uses, or operates
31 systems and assets, whether physical or virtual, vital to the Republic of the Philippines,
32 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, software, and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.

(m) *Defense-CERT* refers to the national coordinating CERT for AFP-CERTS and state sponsored cybersecurity incidents.

(n) *Government computer emergency response team (GCERT)* refers to a specialized trusted team within a government agency that manages, coordinates, and responds to cybersecurity incidents, vulnerabilities, and threats.

(o) *Information and communications technology (ICT)* refers to the totality of electronic means to access, create, collect, store, process, receive, transmit, present, regulate, and disseminate information.

- (p) *Information security* refers to the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- (q) *Integrity of information* refers to the assurance that information and systems are protected against unauthorized modification.
- (r) *National computer emergency response team (NCERT)* refers to a unit under the National Cybersecurity Agency responsible for performing CERT functions and coordination among all CERTs. It is the primary coordinating center for all CERTs.
- (s) *National cyber intelligence network (NCIN)* refers to the inter-agency network managed by the National Intelligence Coordinating Agency (NICA) responsible for the collection, fusion, analysis, coordination and dissemination of strategic and operational cyber intelligence concerning cyber threats to national security, counterintelligence in cyberspace, and the attribution of state-sponsored cyber-attacks.
- (t) *National Security Operations Center (NSOC)* refers to an operations center housed within the NCSA for centralized monitoring, threat detection, and incident response for government agencies to enhance national cybersecurity. It shall monitor critical information assets in cyberspace and conduct baseline assessment of government agencies' cybersecurity posture.
- (u) *Non-repudiation* refers to the ability to prove the occurrence of a claimed event or action and its originating entities.
- (v) *Organization computer emergency response team (ORG-CERT)* refers to responds to cybersecurity incidents within an organization, regardless of their complexity or criticality, while other coordinating CERTS such as the NCERT or SCERT, shall provide specialist support and information to the organization CERT.
- (w) *Public Key Infrastructure (PKI)* refers to a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. The PKI includes the hierarchy of certificate authorities that allow for the deployment of digital certificates that support encryption, digital signature and authentication to meet business and security requirements.
- (x) *Privacy* refers to an individual's rights to exercise control over the collection, access, use and disclosure of his or her personal information held by the government or the private sector.

(y) *Regional Chief Information Security Officer (RCISO)* refers to a cybersecurity official designated by the NCSA, in coordination with the Department of Information and Communications Technology (DICT), with specific role created for government agencies, government-owned and -controlled corporations (GOCCs), and other covered entities that are unable to create a dedicated *plantilla* position for an Individual CISO. They can also be referred to as Group CISO under this Act.

(z) *Responsible disclosure* refers to the practice of not disclosing the vulnerability until the CII responsible for the hardware or software deals fixes the vulnerability.

(aa) *Sectoral computer emergency response team (SCERT)* refers to a coordinating CERT for CIIS, created for administrative or regulatory agencies that oversee the operations of CII sectors.

(bb) *Security Operations Center (SOC)* refers to the focal point for security operations and computer network defense of an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner.

CHAPTER II

THE NATIONAL CYBERSECURITY AGENCY

SEC. 6. *Creation of the National Cybersecurity Agency.* – There is hereby created a National Cybersecurity Agency (NCSA), which shall be under the Department of Information and Communications Technology.

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

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

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

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

3 (a) Policy Planning and Coordination

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

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

1 (c) Cyber Threats and Incidents Response

- 2 (1) Establish the NCERT and a robust incident response capability to promptly detect,
3 analyze, and mitigate cybersecurity incidents involving information technology (IT)
4 systems, OT, and ICS affecting national security or public interest and to
5 collaborate with relevant government agencies, private sector entities, and
6 international partners for coordinated incident response;
- 7 (2) Enhance cybersecurity threat intelligence and situational awareness through the
8 establishment of information-sharing protocols between the NCSA and
9 government agencies;
- 10 (3) Establish a liaison network of CERTs or CERTs Points of Contact, among
11 government agencies to support the implementation of the mandate of NCERT;
- 12 (4) Perform vulnerability assessment and penetration testing initiatives on IT, OT, and
13 ICS, to detect, identify, and analyze cybersecurity threats and to coordinate with
14 law enforcement authorities for the proper attribution of cyber-attacks against CII's;
- 15 (5) Determine the nature and classification of cyber threats and refer incidents to
16 appropriate agency, including, but not limited to the NICA, AFP, Department of
17 Justice (DOJ), and the National Privacy Commission (NPC), Philippine National
18 Police (PNP), National Bureau of Investigation (NBI) and Cybercrime Investigation
19 and Coordinating Center (CICC); and
- 20 (6) Collect open-source data strictly for technical threat intelligence, vulnerability
21 assessment, and cybersecurity incident prevention or response, excluding content
22 regulation, opinion monitoring, or speech analysis, and only insofar as such data
23 is necessary to address a material cybersecurity threat.

24 (d) Research and Development

- 25 (1) Lead and support research and development (R&D) efforts focused on new and
26 emerging cybersecurity technologies, tools, and standards, in partnership with the
27 academe, other government research institutions, and international partners; and
- 28 (2) Study and recommend to Congress fiscal and non-fiscal incentives including tax
29 credits and grants, to encourage and support private sector research and
30 development efforts in cybersecurity technologies and solutions.

1 (e) Capacity Building

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

18 (f) Information Sharing

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

1 (g) International Cooperation

- 2 (1) Foster international collaboration and cooperation for the promotion of
3 cybersecurity including through formal agreements that enhance shared defense,
4 capacity-building, and threat intelligence exchange;
5 (2) Support the government's efforts to establish the Philippines as a regional digital
6 hub; and
7 (3) Provide support to the Department of Foreign Affairs (DFA), as the lead for all
8 international representations, on matters concerning international cybersecurity
9 cooperation.

10 (h) Establish, categorize, and maintain a registry of identified cybersecurity risks and
11 threats.

12 (i) Regulation and Referral

- 13 (1) Recommend to the DOJ the prosecution and imposition of penalties specified
14 under Chapter VI of this Act;
15 (2) Exercise such other powers as may be provided by law, as well as those which
16 may be implied from, or which are necessary or incidental to the carrying out of the
17 express powers granted the NCSA to achieve the objectives and purposes of this
18 law: *Provided, however,* That the regulatory authority of the NCSA shall be
19 ancillary to any duly constituted regulatory jurisdiction granted to any agency by
20 existing laws, such as but not limited to, the NPC, BSP, *et al.*: *Provided, further,*
21 That reasonable notice to, and coordination with the appropriate regulatory agency
22 shall be made by the NCSA prior to the enforcement of the provisions of this Act.
23 Unless expressly specified, nothing in this Act shall be constructed as to diminish
24 or deprive the regulatory jurisdiction conferred by law upon other government
25 agencies concerning the service that they regulate;
26 (3) The NCSA shall have the authority to endorse such matter to the appropriate
27 member-agency or competent authority for proper investigation, enforcement, or
28 prosecution, as may be warranted, upon finding reasonable grounds to believe that
29 additional violations have been committed falling within the jurisdiction of such
30 agency in the course of its investigation. The concerned agency shall take
31 appropriate action in accordance with its mandate, without prejudice to the
32 concurrent powers and proceedings of the NCSA under this Act; and

(4) The NCSA shall perform all other acts as may be necessary to effectively implement the provisions of this Act and to issue orders, resolutions or decisions, including the imposition of administrative sanctions, fines, or penalties, for violations of this Act.

(j) **Cybersecurity Certification**

(1) The NCSA shall promulgate rules and procedures for certifying cybersecurity trustworthiness of service, suppliers, or technologies. Towards this end, the NCSA, in consultation with other government agencies and the private sector, shall devise a rating or scoring system for assessing information security and cybersecurity 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: *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

1 a cybersecurity, information privacy, or information security professional, and has at
2 least a Master's Degree in Cybersecurity, Information Security, or any other related
3 master's degree.

- 4 (b) Deputy Directors-General – The Deputy Directors-General of the NCSA shall be
5 appointed by the President. No individual shall be appointed Deputy Directors-General
6 of the NCSA unless such person is a Filipino citizens domiciled in the Philippines, of
7 good moral character, possessing proven integrity, and unquestionable integrity, with
8 a track record of leadership, recognized competence with the appropriate educational
9 background in cybersecurity or any related field, with at least six (6) years of
10 supervisory or management experience in the field of cybersecurity, data privacy,
11 information technology (IT), IT risk management, or any combination thereof.

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

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

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

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

27 The NCSA shall be under the DICT for policy and program coordination, and shall continue
28 to operate and function laterally and in accordance with prevailing laws:

- 29 (a) All powers and functions related to cybersecurity, including but not limited to the
30 formulation of the National Cybersecurity Plan, establishment of the NCERT, and the
31 facilitation of international cooperation on intelligence regarding cybersecurity matters,
32 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 cybercrime.

(a) The NCERT, which is within the authority of the NSCA, shall work within a strict chain of command with all other CERTs. It shall also coordinate their efforts with the Defense-cert as the national coordinating CERTs.

(b) The NSCA, through the NSOC, shall send data and threat information to the National Cybersecurity Intelligence Network (NCIN), a cyber fusion center operated by the NICA, so that it can process and provide actionable intelligence and important situational awareness to both the NCERT and the Defense-cert.

(c) The NCSA, upon determination that a series of cybersecurity incidents are attributable to a state-sponsored threat actor, shall hand over the response activities to the Defense-cert.

(d) The NCSA, upon determination that a cybercrime is present in an incident they are responding to, shall escalate the matter for proper turn-over to The Philippine National Police Anti-Cybercrime Group or the National Bureau of Investigation-Cybercrime Division.

CHAPTER III

CRITICAL INFORMATION INFRASTRUCTURE

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

- 1 (a) The NCSA shall identify entities that own, operate or maintain CII using a risk-based
2 approach, as prescribed by the NCSP and shall adopt a set of criteria for
3 identifying CII.
- 4 (b) After the confirmation of the CII designation, the NCSA shall issue a written notice to
5 the owner of the computer or computer system, designating said system as a CII for
6 the purposes of this Act.
- 7 (c) A notice issued under subparagraph (a) shall:
- 8 (1) Identify the computer or computer system that is being designated as a CII;
9 (2) Identify the owner of the computer or computer system so designated as a CII;
10 Inform the owner of the computer or computer system, regarding the owner's
11 duties and responsibilities under this Act that arise from the designation; and
12 (3) Inform the owner of the computer or computer system that any representation
13 against, or a decision on the designation, may be challenged and to provide
14 information on the applicable procedure.
- 15 (d) Any designation under subparagraph (a) shall be in effect for a period of five (5) years,
16 unless it is withdrawn by the NCSA before the expiration of the period.

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

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

23 **SEC. 18. Compliance Requirements for Organizations and the CII.** – The NCSA
24 shall, in coordination with concerned government regulatory agencies, create a list of compliance
25 requirements for CII. In determining the compliance requirements for organizations and CII,
26 due consideration shall be given to minimizing their impact on the cost of services provided by
27 the organizations and CII. These shall include the following:

- 28 (a) List of authorized personnel and their level of access to the computer system labeled
29 as CII;
- 30 (b) The cybersecurity or information security framework used for risk assessment and
31 adoption of technical and procedural controls;
- 32 (c) Initial audit report;

- (d) Cybersecurity incident handling organization and protocol being implemented by the CII operator;
- (e) Organization and technical contact persons of the CII operators;
- (f) The OT or ICS utilized, when applicable; and
- (g) Such other information, as may be required by the NCSA.

SEC. 19. Cybersecurity Audit and Risk Assessment of CII. – All CII operators shall take the necessary steps to identify, assess, and institute technical or procedural controls to mitigate cybersecurity risks related to the CII at least once every three (3) years.

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

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

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

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

SEC. 21. Assistance Extended by the Government to CII Operators. – Operators of CII may request assistance for NCSA to provide the following:

- (a) Use of government technical controls and systems for the defense and protection of the CII;
- (b) Priority co-location with government data centers subject to availability;

(c) Use of government secure crypto-primitives such as but not limited to, digital certificates; and

(d) Knowledge management platform to facilitate faster sharing of information between the industry, NCSA, government regulators, and other concerned organizations.

SEC. 22. Confidentiality of CII Related Documents. – The official list of CIIs, including the assessment, evaluation, audit, and technical reports shall be considered documents related to National Security and thus, are considered confidential and classified. The proper authority by law, administrative or legal order, and upon the recommendation of NCSA, may declassify these documents.

If a *subpoena duces tecum* is issued for any of these classified documents, NCSA shall inform the body who ordered the subpoena that the document can only be opened or scrutinized in an executive session and shall be disclosed only to a limited number of people on a strict need-to-know basis.

SEC. 23. Withdrawal or Removal of CII Designation. – The NCSA, through a written resolution, may withdraw or remove the designation of any CII at any time if the NCSA is of the opinion that the computer or computer system no longer fulfills the criteria of a CII. The NCSA shall notify in writing the CII operator of the withdrawal or removal of such designation within fourteen (14) days from the issuance of the resolution.

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 DBM and CSC.

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

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

CHAPTER V

PROHIBITED ACTS AND PENALTIES

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

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

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

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

(b) Administrative Liability of CII Operators. – Upon determination of a violation of this Act, its implementing rules and regulations, or other relevant issuances, the NCSA may impose the following:

(1) A fine of at least Five thousand pesos (Php 5,000.00) but not exceeding Two million pesos (Php 2,000,000.00) per violation: *Provided*, That if the CII operator has a gross annual income not exceeding Ten million pesos (Php 10,000,000.00), the imposable penalty shall be equivalent to one percent (1%) to two percent (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 VI
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 come from the existing Secretariat personnel of the Committee on Science and Technology of the Senate and the Committee on Information and Communications Technology of the House of Representatives.

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

SEC. 33. Report. – The NCSA shall submit an annual report to the Office of the President on the implementation of this Act, as well as the operations of the NCSA. The NCSA shall also include in its report disclosures of cybersecurity vulnerabilities, actionable protocols to mitigate

1 cybersecurity vulnerabilities to information systems and industrial control systems. The NCSA
2 shall likewise publish a “State of Cybersecurity in the Philippines” report for covered entities and
3 the general public.

4 **SEC. 34. Confidentiality. –**

5 (a) All parties involved in the application of this Act shall respect the confidentiality of
6 information and data obtained in carrying out their tasks and activities in such a manner
7 as to protect, in particular:

8 (1) Intellectual property rights, and confidential business information or trade secrets
9 of a natural or juridical person, including source code, except in cases where the
10 disclosure and access is necessary to protect the legitimate interest recognized
11 by existing laws, rules, and regulations;

12 (2) Public and national security interests;

13 (3) Data of security agencies, ensuring that they will not be migrated into the private
14 domain; and

15 (4) Integrity of criminal or administrative proceedings.

16 (b) Without prejudice to paragraph (a), information exchanged on a confidential basis
17 between government departments, agencies, bureaus, offices, and institutions and the
18 NCSA shall not be disclosed without the prior agreement of the originating
19 government departments, agencies, bureaus, offices, and institutions.

20 (c) Adequate protection shall be set in place between the information shared by the
21 private sector and government agencies, particularly security and law enforcement
22 agencies.

23 (d) Paragraphs (a) and (b) shall not affect the rights and obligations of the NCSA and
24 notified bodies with regard to the exchange of information and the dissemination of
25 warnings, nor the obligations of the persons concerned to provide information under
26 existing laws, rules, and regulations.

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

30 **SEC. 35. Periodic Review. –** The NCSA, in consultation with the DICT, the DOST, and
31 other concerned agencies shall conduct a review of the Act every three (3) years, or more
32 frequently as may be necessary, to ensure that certifications, regulations, standards, penalties,
33 and other provisions of the Act, with the end in view of meeting the cybersecurity standards and
34 requirements for emerging technologies.

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

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

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

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

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

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

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

23 **SEC. 40. Repealing Clause.** – All laws, presidential decrees, executive orders, letters of
24 instructions, proclamations, or administrative regulations that are inconsistent with the provisions
25 of this Act are hereby repealed, amended, or modified accordingly.

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

Approved,