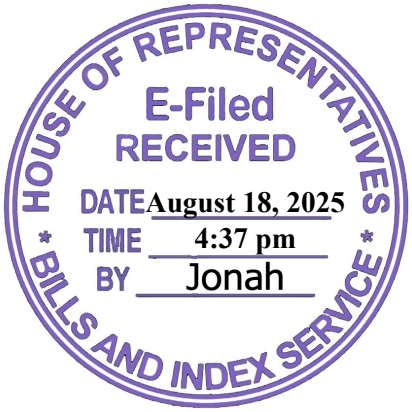
Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

House Bill No. 3822



Introduced by **REP. JAVIER MIGUEL L. BENITEZ**

EXPLANATORY NOTE

The Philippines faces mounting cybersecurity challenges, with rising incidents of data breaches, online fraud, and critical infrastructure attacks that threaten both public safety and economic stability. The absence of a comprehensive cybersecurity law creates a critical gap in the national legal framework, undermining the country's capacity to deter, prevent, and respond to increasingly sophisticated cyber threats. Without clear legal measures, our digital infrastructure remains exposed, jeopardizing not only national security but also the trust and integrity essential for economic growth in the digital age.

In September 2023, the Medusa ransomware attack on the Philippine Health Insurance Corporation (PhilHealth) compromised the personal data of at least 13 million members and nearly 800 employees, marking one of the most severe data breaches in Philippine history.[1] This was not an isolated case: similar intrusions have targeted the Philippine Statistics Authority, the Department of Science and Technology, and even the websites of both Chambers of Congress. The private sector is equally at risk. Cisco's 2025 Cybersecurity Readiness Index reports that eighty-five (85) percent of Philippine companies experienced AI-related cyberattacks in 2024, while only six (6) percent have reached a "mature" stage of readiness to defend against such threats.[2] These incidents reveal systematic vulnerabilities across sectors that, if left unaddressed, jeopardize economic stability, national security, and public safety.

[1] Jaymalin, M. (October 18, 2023). PhilHealth: 13 million members affected by data breach. The Philippine Star. https://www.philstar.com/headlines/2023/10/19/2304835/philhealth-13-million-members-affected-data-breach. (Date last accessed: August 11, 2025).
[2] Adonis, M. (May 9, 2025). 85% of Philippine companies grapple with cyber threats –Cisco. Philippine Daily Inquirer. https://business.inquirer.net/524497/85-of-ph-companies-grappled-with-cyber-threats-in-24-cisco. (Date last accessed: August 11, 2025).

Cyberattacks on critical infrastructure such as power grids, healthcare systems, transportation networks, and government databases can cripple essential services, undermine public trust, and compromise national sovereignty. The current fragmented and reactive approach to cybersecurity leaves both government and industry ill-prepared to respond to increasingly sophisticated threat actors.

To confront these escalating threats and to bridge this concerning gap in our country, the proposed measure establishes the National Cybersecurity Agency (NCSA) as the primary policy, planning, and implementing authority for safeguarding the nation's Critical Information Infrastructure ("CII"). It mandates a unified national cybersecurity strategy anchored on a Zero Trust Architecture and aligned with international standards, while ensuring strong coordination among government agencies, the private sector, and international partners. The bill further prescribes baseline cybersecurity requirements across the public sector, provides for the designation and regulation of CII entities, institutionalizes incident reporting and rapid response protocols, and imposes strict penalties for non-compliance and for unauthorized disclosure of classified information.

In accordance with the State's constitutional mandate to "Serve and protect the people"[3] and to secure its sovereignty, territorial integrity, and the general welfare,[4] the passage of this measure is imperative. It will fortify the Republic's cyber defenses, safeguard essential services from debilitating attacks, and position the Philippines as a resilient and trusted hub in the digital age.

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

JAVIER MIGUEL L. BENITEZ

[3] 1987 Constitution, Article II, Section 4.
[4] 1987 Constitution, Article II, Section 5.

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
First Regular Session

House Bill No. 3822

Introduced by **REP. JAVIER MIGUEL L. BENITEZ**

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

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

CHAPTER I
GENERAL PROVISIONS

SECTION 1. ***Short Title.*** **–** This Act shall be known as the "*Cybersecurity Act*."

SEC. 2. ***Declaration of Policy.*** **–** It is hereby declared a policy of the State:

(a) To recognize the vital role of communications and information in nation-building;

(b) To recognize the maintenance of peace and order, the protection of life, liberty, and property, and the promotion of the general welfare are essential for the enjoyment by all the people of the blessings of democracy;

(c) To serve and protect the people, and as the Constitution guarantees the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizure, and that the privacy of communication and correspondence shall be inviolable except upon lawful order

of the court, cybersecurity and information security are important to the protection of the Filipino society;

(d) To adopt measures to effectively prevent and combat cybersecurity offenses by facilitating detection, investigation, and prosecution of offenses at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation; and

(e) To adopt a Zero Trust Architecture in cybersecurity, as appropriate in the Philippine context and aligned with international standards and best practices.

SEC. 3. ***Definition of Terms.*** **–** For purposes of this Act, the following terms shall mean:

(a) *Availability* – refers to the property of being accessible and usable upon demand by an authorized entity.

(b) *Computer Network* – refers to a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless.

(c) *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.

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

(e) *Critical Information Infrastructure (CII)* – refers to a computer or a computer system located wholly or partly in the Philippines, necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in the Philippines. CIIs consist of information process and

information and communications technology which form part of the operation of the critical infrastructures.

(f) *Critical infrastructure (CI)* – refers to any public service which owns, uses, or operates systems and assets, whether physical or virtual, so vital to the Republic of the Philippines that the incapacity or destruction of such systems or assets would have a detrimental impact on national security, including telecommunications and other such vital services as may be declared by the President of the Philippines.

(g) *Cryptographic primitive crypto-primitive* – refers to a low-level cryptographic algorithm used as a basic building block for higher-level cryptographic algorithms.

(h) *Cybercrime* – encompasses illegal activities conducted within cyberspace which may involve malicious intent. Involves activities violating laws and regulations such as the Cybercrime Prevention Act (Republic Act No. 10175, as amended), resulting in severe consequences such as privacy breaches, disruption of critical services.

(i) *Cybersecurity* – refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

(j) *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.[5]

(k) *Information and communications technology (ICT)* – encompasses all technologies for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and information.

(l) *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.

(m) *Integrity* – refers to the property of accuracy and completeness.

---

[5]National Cybersecurity Plan 2023-2028, p xii

(n) *National Computer Emergency Response Team (NCERT)* – refers to a group of information security experts and practitioners responsible for responding to cybersecurity incidents of an organization with the aim of minimizing the impact or damage and ensuring recovery of affected systems.

(o) *Non-Repudiation* – refers to the ability to prove the occurrence of a claimed event or action and its originating entities.[6]

(p) *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.

(q) *Privacy* – refers to having the personal control over personal information.[7]

(r) *Protective Domain Name System (PDNS)* – refers to the naming database that locates, tracks, and regulates internet domain names and IP addresses.

(s) *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.

(t) *Zero Trust (ZT)* – refers to an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users and resources. It is a set of security primitives rather than a particular set of technologies. Zero trust assumes that there is no implicit trust granted to user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or to endpoints (devices) based on their ownership (e.g., enterprise or personally owned). Zero trust focuses on protecting resources (e.g., devices, services, workflows, network accounts) rather than network segments, as the network location is no longer seen as the prime component to the security posture of the resource.

---

[6]National Cybersecurity Plan 2023-2028, pp xiii

[7]National Cybersecurity Plan 2023-2028, pp xiii

(u) *Zero Trust Architecture (ZTA)* – refers to an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

CHAPTER II
ORGANIZATION OF THE NATIONAL CYBERSECURITY AGENCY

SEC. 4. *Creation of the National Cybersecurity Agency ("NCSA").* – There is hereby created a NCSA, which shall be an attached agency to the Department of Information and Communications Technology ("DICT").

SEC. 5. *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.

SEC. 6. The Agency shall exercise the following powers and functions:

(a) Policy Planning and Coordination:

(i) Formulate policies and recommendations on issues concerning cybersecurity, advise Congress and other government agencies on all aspect of cybersecurity, and propose legislation and amendments thereto;

(ii) Formulate and implement the National Cybersecurity Plan;

(iii) Ensure the participation of all stakeholders in policy formulation and implementation;

(iv) Lead the whole-of-government effort to formulate cybersecurity regulations, in accordance with international standards and best practices;

(v) Set national standards on the generation, management, use, optimization, and, if applicable, disposal of cybersecurity products, protocols, and crypto-primitives such as, but not limited to: Public Key Infrastructures (PKI); secure routing protocols; secure network elements; protective Domain Name Service; encryption and decryption protocols, and authentication protocols;

(vi) Coordinate all cybersecurity activities of the government, in partnership with the private sector and other stakeholders;

(vii) Advise the President, Congress, Judiciary, and Constitutional bodies on all cybersecurity-related issues and concerns;

(viii) Create the National Vulnerability Disclosure Program. The program shall be the gateway for the security researchers to submit vulnerabilities of the online assets of the Philippine government;

(b) CII Protection:

(i) Formulate and set cybersecurity minimum standards for CIIs, in coordination with relevant administrative agencies exercising regulatory functions over CIIs;

(ii) Ensure compliance of CIIs to cybersecurity minimum standards requirements;

(iii) Conduct audit and assessment of the cybersecurity posture of CIIs, all National Government Agencies, including Government-Owned and/or Controlled Corporations (GOCCs), State Universities and Colleges (SUCs), and Local Government Units (LGUs). The Congress and the Judiciary may request the NCSA to assist them in the conduct of cybersecurity audit and assessment;

(iv) Establish a liaison network of CERTs (or CERTs Points of Contact) among CIIs to facilitate communication and information sharing;

(v) Regulate and provide oversight over private cybersecurity service providers such as, but not limited to Vulnerability Assessment and Penetration Testing (VAPT) service providers, security operations center providers, etc.;

(vi) 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;

(c) Cyber Threats and Incidents Response:

(i) Establish the NCERT and a robust incident response capability to promptly detect, analyze, and mitigate cyber incidents affecting national security

or public interest and to collaborate with relevant government agencies, private sector entities, and international partners for coordinated incident response;

(ii) Enhance cyber threat intelligence and situational awareness;

(iii) Establish a liaison network of CERTs (or CERTs Points of Contact) among government agencies to support the implementation of the mandate of NCERT;

(iv) Perform vulnerability assessment and penetration testing initiatives to detect, identify, and analyze cyber threats and to properly attribute cyber-attacks against CIIs;

(v) Initiate legal proceedings for the collection of computer data and summon witnesses to appear in any proceedings, investigation, or inquiry of the NCSA regarding cybersecurity incidents of national government agencies (NGAs) and instrumentalities, and CII;

(vi) Collect open source data and conduct data analysis for proactive cybersecurity measures against misinformation, deceptive content, and other forms of attacks on integrity of information;

(d) Research and Development:

(i) Lead in the development of cybersecurity technologies, tools, and standards, in partnership with the academe, other government research institutions, and international partners;

(e) Capacity Building:

(i) Develop and implement training programs to build and maintain a highly skilled cyber workforce in the government;

(ii) Partner with academic institutions, industry stakeholders, and foreign counterparts to promote knowledge sharing, resource sharing, and skills development in cybersecurity;

(iii) Prescribe personnel qualifications and other qualification standards essential to the effective development on cybersecurity field of expertise;

(iv) Co-develop with the Civil Service Commission (CSC) the cybersecurity qualification standards;

(f) Information Sharing:

(i) Gather, assess, and distribute actionable intelligence regarding cyber threats, emerging patterns, and potential vulnerabilities, thereby bolstering the nation's cyber situational awareness and facilitating informed decision-making processes;

(ii) Develop a mechanism for information-sharing between the government (or public) and the private sector;

(iii) Issue cybersecurity advisories or guidelines regularly or as needed;

(g) International Cooperation:

(i) Foster international collaboration and cooperation for the promotion of cybersecurity;

(ii) Support the government's efforts to establish the Philippines as a regional digital hub;

(iii) Represent the Republic of the Philippines, in coordination with other relevant agencies in international cybersecurity cooperation;

(h) Regulatory:

(i) In any investigation under Chapter 6: Prohibited Acts, after due notice and hearing, the NCSA may impose sanctions, collect fees, fines, and penalties for the violation of laws, rules, regulations, orders, and issuances on CIIs; and

(ii) Exercise such other powers as may be provided by law, as well as those which may be implied from, or which are necessary or incidental to the carrying out of the express powers granted the NCSA to achieve the objectives and purposes of this law.

SEC. 7. ***Composition.*** **–** The NCSA shall be headed by a Director-General with the rank of Undersecretary and shall be assisted by two Deputy Directors-General with the rank of Assistant Secretaries.

SEC. 8. ***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 he or she is a citizen residing in the Philippines for the past 10 years, 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 they are citizens residing in the Philippines for the past 10 years, of good moral character, possessing proven integrity, and having 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. 9. ***Separation and Retirement from Service.*** **–** Employees who are separated from service within six (6) months from the effectivity of this Act as a result of the consolidation and/or reorganization under the provisions of this Act shall receive separation benefits to which they may be entitled under Executive Order No. 366, s. 2004. Those who are qualified to retire under existing retirement laws shall be allowed to retire and receive retirement benefits to which they may be entitled under applicable laws and issuances.

SEC. 10. ***Structure and Staffing Pattern.*** **–** Subject to the approval of the Department of Budget and Management (DBM), NCSA shall determine its organizational structure and create new divisions or units as it may deem necessary. The NCSA shall appoint officers and employees in accordance with the civil service law, rules, and regulations.

(a) Considering the highly technical nature of the personnel required for the NCSA, the NCSA may promulgate a separate set of qualification and competency standards for eligibility as career officers in NCSA. The NCSA qualification and competency standards shall only be applicable to NCSA unless adopted by the CSC as applicable for the entire Philippine government; and

(b) The NCSA may request detail of personnel from other government departments, agencies, bureaus, offices, and institutions, subject to the approval of the head of office and availability of personnel, to ensure the effective coordination, integration, and fusion of activities relative to cybersecurity.

SEC. 11. ***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 is hereby attached to the DICT 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; and

(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.

(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 Section 11 of this Act, 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.

CHAPTER III
CRITICAL INFORMATION INFRASTRUCTURES (CII)

SEC. 12. ***Designation of Critical Information Infrastructure (CII).*** **–** The NCSA will have the duty and power to oversee the CIIs in the Philippines.

(a) The NCSA shall identify entities that own, operate or maintain CII ("CII entities" from hereon), using a risk-based approach, as prescribed by the NCSP and shall adopt a set of criteria for identifying CIIs.

(b) After the confirmation of the CII designation, the NCSA will issue a written notice to the owner of the computer or computer system, designating said system as a CII for the purposes of this Act.

(c) A notice issued under subparagraph I must:

(i) Identify the computer or computer system that is being designated as a CII;

(ii) Identify the owner of the computer or computer system so designated as a CII;

(iii) Inform the owner of the computer or computer system, regarding the owner's duties and responsibilities under this Act that arise from the designation;

(iv) Inform the owner of the computer or computer system that any representations against the designation are to be made to the NCSA by a specified date, being a date not earlier than fourteen (14) days after the date of the notice; and

(v) Inform the owner of the computer or computer system that the owner may appeal to the NCSA against the designation, and provide information on the applicable procedure.

(d) Any designation under Subsection I shall be in effect for a period of five (5) years, unless it is withdrawn by the NCSA before the expiration of the period.

SEC. 13. ***Regulation of providers of essential services who rely on third-party owned CII.*** **-** Providers remain responsible for the cybersecurity and resilience of the computer systems they rely on to deliver essential services, even if those systems are managed by a third party. Providers who depend on third-party-owned CII must secure legally binding commitments from these vendors

ensuring that the third party meets the cybersecurity standards and requirements applicable to CII, including incident reporting, auditing, and risk assessment.

SEC. 14. ***Compliance requirements for organizations and the CIIs.*** **–** The NCSA, in coordination with concerned government regulatory agencies, shall create a list of compliance requirements for CIIs. In determining the compliance requirements for organizations and CIIs, due consideration shall be given to minimizing their impact on the cost of services provided by the organizations and/or CIIs. These shall include at least the following:

(a) List of authorized personnel and their level of access to the computer system labeled as CII;

(b) List of supply chain service providers of the CII including foreign service providers, if any;

(c) The cybersecurity or information security framework used for risk assessment and adoption of technical and procedural controls;

(d) Initial audit report;

(e) Cybersecurity incident handling organization and protocol being implemented by the CII operator; and

(f) Organization and technical contact persons of the CII operators.

SEC. 15. ***Cybersecurity Audit and Risk Assessment of CIIs.*** **–** 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.

SEC. 16. ***Mandatory Disclosure of Cybersecurity Incidents on CIIs.*** **–**

(a) Organizations operating CIIs shall notify the government regulator and NCSA through the NCERTupon discovery of a critical or high-risk cybersecurity incident. 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;

(b) In the event of ransomware or extortion attacks, 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

(c) CERTs shall coordinate with law enforcement agencies in filing of cybercrime cases.

SEC. 17. ***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; and

(c) Use of government secure crypto-primitives such as digital certificates, etc.; and

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

SEC. 18. ***Confidentiality of CII Related Documents.*** **–** The official list of CIIs, including their assessment, evaluation, audit, and technical reports shall be considered documents related to National Security and thus, are considered confidential and classified. The President, 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 executive session, and/or shall be disclosed only to a limited number of people on a strict need-to-know basis.

SEC. 19. ***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 their designation within 14 days upon the issuance of the resolution.

SEC. 20. ***Motion for Reconsideration of CII Certification.*** **–** CIIs may file for motion for reconsideration of the scoring or rating, and revocation of certificate to NCSA within thirty (30) days from the receipt of the decision.

CHAPTER IV
MINIMUM CYBERSECURITY REQUIREMENTS

National Government Agencies (NGA) and instrumentalities, Government-Owned and -Controlled Agencies (GOCC), and Local Government Units (LGU) are hereby directed to adopt and implement minimum cybersecurity requirements to enhance their resilience against cyber threats.

SEC. 21. ***Prescribing Minimum Cybersecurity Requirements***. – The NCSA, in consultation with relevant stakeholders, shall prescribe a baseline for security practices, ensuring a consistent level of protection across government agencies. As may be necessary, the NCSA, in cooperation with the private sector, shall provide technical assistance to other government agencies and offices relative to this provision.

SEC. 22. ***Creation of a Chief Information Security Officer (CISO).*** **–** Each NGA, GOCC, and LGU shall create a CISO position within the agency to lead the Government Computer Emergency Response Team (GCERT). The CISO shall be the official responsible for carrying out the Chief Information Officer responsibilities and serve as the primary liaison to the agency's authorizing officials, information system owners, information system security officers, and the SCERT and the NCERT.

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
CYBERSECURITY IOT CERTIFICATION

SEC. 23. ***Cybersecurity Anchor of Trust System (CATS).*** **–** NCSA shall promulgate rules and procedures for certifying cybersecurity trustworthiness of service, suppliers, or technologies. Towards this end, the Agency 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 Agency.

The Agency may charge reasonable fees to defray the administrative cost of the services rendered, subject to existing laws and regulations.

SEC. 24. ***Voluntary Rating System.*** **–** Any local or foreign commercial entities may voluntarily submit themselves for certification.

SEC. 25. ***Validity of Certification.*** **–** 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 Agency, 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. 26. ***Cybersecurity IoT Certification Appeal.*** **–** Agencies with cybersecurity IoT certification may file for an appeal of the scoring or rating, and revocation of certificate to NCSA within thirty (30) days from receipt of the decision.

CHAPTER VI
PROHIBITED ACTS AND PENALTIES

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. ***Disclosure of Confidential Information.*** **–** Any individual who has access to CII and information is prohibited to disclose them. The unauthorized disclosure of these confidential information, either willfully or through negligence, shall be penalized.

SEC. 29. ***Penalties.*** **–** The following penalties shall be applied for violations of this Act:

(a) Any individual who either willfully, or through negligence causes the unauthorized disclosure of confidential or sensitive information shall be penalized by imprisonment ranging from six (6) years to twelve (12) years or a fine of not less than Five hundred thousand pesos (P 500,000.00), or both;

(b) Any unauthorized disclosure of confidential or sensitive information affecting national defense or national security, with intent or reason to believe that the same is to be used to the injury of the Philippines or to the advantage of any foreign nation or enemy of the State, whether domestic or foreign, shall suffer the penalty of life imprisonment or by a fine of not less than One million pesos (P 1,000,000.00), or both;

(c) Any employee who leaves or severs employment with the CII operator/owner, willfully or negligently discloses, damages, disposes of, or destroys critical, sensitive, or classified information in violation of this Act and other existing laws, rules, and regulations, contravenes or fails to comply with any provision of this Act shall be held liable without prejudice to any criminal prosecution;

(d) Upon violation of any enumerated prohibited acts, the CII operator shall receive a formal written warning from the NCSA ordering the CII to show cause within seven (7) days from receipt thereof;

(e) If the CII operator fails to comply with the written warning, NCSA shall impose a fine equal to half of one percent (0.5%) of the CII operator's average gross annual income for a period of five years. An additional half of one percent (0.5%) shall be added for each subsequent infraction, with the penalty resetting after the CII operator finally complies with the directives;

(f) A CII operator's willful disregard of a lawful order given by NCSA to comply with this Act and its implementing rules and regulations within a reasonable time frame will result in the CII operator's license being revoked on grounds of non-compliance to a regulatory requirement;

(g) The CII operator has the right to appeal any penalties imposed under this section. To initiate an appeal, the CII operator must submit a written notice of appeal to the NCSA within fifteen (15) days from the receipt of the penalty notice or the revocation order. The appeal must include a detailed statement of the grounds for contesting the penalty and any supporting evidence. Upon receipt of the appeal, the NCSA shall review the case and may hold a hearing if

deemed necessary. The CII operator will be notified of the hearing date and will have the opportunity to present their case. Following the review or hearing, the NCSA will issue a written decision on the appeal. The decision of the NCSA shall be final and may be challenged only through appropriate judicial review, as provided by applicable law.

SEC. 30. ***Liability under the Anti-Terrorism Act (ATA) of 2020.*** **–** Any person who, within or outside the Philippines, regardless of the stage of execution, engages in acts intended to cause extensive interference with, damage, or destruction to Critical Infrastructure, as defined under Section 3 (f) of this Act or Section 3 (a) of Republic Act No. 11479, Section 2 (e) of Republic Act No. 11659, or Section 3 (j) of Republic Act No. 10175, or to CIIs designated under Chapter 3 of this Act, or under other applicable laws on Critical Infrastructure and CIIs, whether committed by, through and with the use of information and communications technologies or otherwise, when the purpose of such act, by its nature and context is to intimidate the general public or a segment thereof, create an atmosphere or spread a message of fear, to provoke or influence by intimidation the government or any international organization, or seriously destabilize or destroy the fundamental political, economic, or social structures of the country, or create a public emergency or seriously undermine public safety, shall be liable under Section 4 (c) of Republic Act No. 11479, otherwise known as the Anti-Terrorism Act of 2020.

CHAPTER VII
MISCELLANEOUS PROVISIONS

SEC. 31. ***Authority to Accept Assistance and/or 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. 32. ***Appropriations.*** **–** The amount necessary for the initial implementation of this Act shall be charged against the current and available appropriations of concerned agencies. Thereafter, the amount needed for the implementation of this Act shall be included in the annual General Appropriations Act.

SEC. 33. ***Cybersecurity Risk Management and Mitigation Fund.*** **–** There is hereby created a Cybersecurity Risk Management and Mitigation Fund (CRMMF).

(a) CRMMF shall be used for cybersecurity risk mitigation, prevention, and preparedness activities such as but not limited to training of personnel,

procurement of equipment, and capital expenditures. It can also be utilized for the management of imminent or actual cybersecurity threats which may occur during the current fiscal year or those that occurred in the past two (2) years from the current fiscal year. Risk management activities include threat identification and detection, incident response, system recovery and protection, and other related works or services;

(b) The specific amount of the CRMMF and the appropriate recipient agencies shall be determined upon approval of the President of the Philippines in accordance with the favorable recommendation of the NCSA;

(c) Of the amount appropriated for the CRMMF, thirty percent (30%) shall be allocated as Quick Response Fund (QRF) or a contingent fund for response and recovery activities in order to immediately bring affected CII systems to normal operation; and

(d)All departments/agencies that are allocated with the CRMMF shall submit to the NCSA their monthly statements on the utilization of CRMMF and make an accounting thereof in accordance with existing accounting and auditing rules.

SEC. 34. ***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 Agency. The NCSA shall also include in its report disclosures of cybersecurity vulnerabilities, actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems.

SEC. 35. ***Confidentiality.***

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

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

(ii) Public and national security interests;

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

(iv) Integrity of criminal or administrative proceedings.

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

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

(d) Paragraphs I and II shall not affect the rights and obligations of the NCSA and 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. 36. ***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. 37. ***Utilization of the collected fees, fines, and penalties.*** **–** The NCSA is hereby authorized to utilize the fees and penalties collected for programs and projects aimed at enhancing cybersecurity capabilities and infrastructure within the jurisdiction. These funds shall be allocated towards initiatives such as cybersecurity awareness campaigns, capacity-building programs, research and development efforts, and the procurement of advanced cybersecurity technologies and tools, provided that at no circumstance shall the funds be used to augment salaries and personnel benefits.

The utilization of the aforementioned fund shall be subject to government accounting manual and audit procedures, ensuring transparency, accountability,

and proper fiscal management in accordance with the objectives and mandates of NCSA. Regular audits and reporting requirements shall be conducted to ensure the effective and efficient utilization of funds.

SEC. 38. ***Implementing Rules and Regulations (IRR).*** **–** Within one hundred twenty (120) days from 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. 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 of this Act are hereby repealed, amended, or modified accordingly.

SEC. 41. Effectivity clause. **–** This Act shall take effect fifteen (15) days following its publication in the Official Gazette or at least two national newspapers of general circulation.

Approved,