

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

TWENTIETH CONGRESS
First Regular Session
House Bill No. 8048



Introduced by Representative
BRIAN POE, PhD, MNSA

**AN ACT ESTABLISHING A COMPREHENSIVE AND CITIZEN-CENTRIC
NATIONAL CYBERCRIME AND SCAM PREVENTION AND RESPONSE
FRAMEWORK, AMENDING RA 10175, AND FOR OTHER PURPOSES**

EXPLANATORY NOTE

Cybercrime has evolved into a direct threat to public trust, economic stability, and national security. While existing laws provided an initial foundation, they are no longer adequate to confront the speed, scale, sophistication, and transnational character of modern cybercrime. This measure introduces targeted reforms to restore control over cyberspace and protect the public and the digital economy.

First, it strengthens penal protections against acts that undermine trust in digital systems, including the malicious refusal to surrender lawfully required data, the solicitation of cybercrime, and large-scale offenses amounting to economic sabotage. These provisions recognize that cybercrime today is not merely individual misconduct, but organized, strategic, and economically destructive.

Second, the measure establishes a stakeholder-centric enforcement framework through the creation of a National Scam Hub, prioritizing the immediate disruption of scam operations and the rapid mitigation and recovery of losses via a tightly integrated, multi-stakeholder response. The co-location of investigators, banks, e-wallet operators, and relevant agencies enables swift, coordinated action before formal complaint processing, significantly enhancing victim protection and investigative efficiency. The measure further liberalizes complaint procedures by empowering service providers and law enforcement officers to initiate cases when

victims are unable to do so — particularly in cross-border and online contexts where delay breeds impunity.

Third, it modernizes the legal framework for digital evidence custody and forensic use, aligning the law with contemporary investigative realities and global best practices while safeguarding due process.

Fourth, it updates and harmonizes existing laws to reflect present-day technologies and criminal structures, including recognizing organized cybercrime groups, expanding the concept of ICT systems to cover IoT and converged platforms, and adopting operationally relevant definitions that reflect how cybercrime is actually committed and facilitated.

Finally, the measure creates a cohesive national response architecture, institutionalizing a National Anti-Cybercrime Strategic Plan, and creating a National Cybercrime Prevention and Investigation Agency to unify enforcement and intelligence under a single, accountable authority.

Together, these reforms shift the country from a fragmented, reactive system to a decisive, coordinated, and technology-driven defense of the public, the economy, and trust in the digital space.


HON. BRIAN POE, PHD, MNSA
Representative
FPJ Panday Bayanihan Party-List

Republic of the Philippines
HOUSE OF REPRESENTATIVES

Quezon City, Metro Manila

TWENTIETH CONGRESS

First Regular Session

House Bill No. **8048**

Introduced by Representative

BRIAN POE, PhD, MNSA

**AN ACT ESTABLISHING A COMPREHENSIVE AND CITIZEN-CENTRIC
NATIONAL CYBERCRIME AND SCAM PREVENTION AND RESPONSE
FRAMEWORK, AMENDING RA 10175, AND FOR OTHER PURPOSES**

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

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

CHAPTER I
PRELIMINARY PROVISION

Section 1. Title. – This Act shall be known as the "Anti-Cybercrime Act of 2026".

Section 2. Declaration of Policy. – The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting electronic commerce, and data processing, in the nation's overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to

protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

IT IS THE POLICY OF THE STATE TO RECOGNIZE THE INDISPENSABLE ROLE OF ICT, INCLUDING BUT NOT LIMITED TO TELECOMMUNICATIONS, BROADCASTING, ELECTRONIC COMMERCE, CONTENT PRODUCTION, AND DATA PROCESSING, IN ADVANCING THE NATION'S SOCIAL, ECONOMIC, POLITICAL, AND CULTURAL DEVELOPMENT. THE STATE SHALL PROMOTE AN ENVIRONMENT THAT IS CONDUCIVE TO THE RESPONSIBLE GROWTH, INNOVATION, AND RATIONAL APPLICATION OF ICT, THEREBY ENSURING FREE, EQUITABLE, AND INTELLIGIBLE ACCESS TO THE EXCHANGE AND DELIVERY OF INFORMATION FOR ALL.

THE STATE LIKEWISE AFFIRMS THE NECESSITY OF PROTECTING AND SAFEGUARDING THE CONFIDENTIALITY, INTEGRITY, AVAILABILITY, AUTHENTICITY, NON -REPUDIATION, PRIVACY, AND SECURITY OF COMPUTER SYSTEMS, COMMUNICATIONS NETWORKS, AND DATABASES. TO THIS END, THE STATE SHALL PENALIZE ALL FORMS OF MISUSE, ABUSE, AND ILLEGAL ACCESS THAT UNDERMINE THE TRUST AND STABILITY OF THE ICT ENVIRONMENT.

THE STATE FURTHER RECOGNIZES THAT THE MISUSE OF ICT AS A TOOL FOR CRIMINAL ACTIVITY ENABLES OFFENDERS TO OPERATE WITH UNPRECEDENTED SPEED, REACH, AND ANONYMITY, THEREBY MAGNIFYING THE DESTRUCTIVE IMPACT OF TRADITIONAL CRIMES AND EMPOWERING ORGANIZED CRIME GROUPS OR SYNDICATES TO VICTIMIZE LARGE SEGMENTS OF THE POPULATION SIMULTANEOUSLY. IN ORDER TO

SAFEGUARD PUBLIC ORDER, NATIONAL SECURITY, AND ECONOMIC STABILITY, THE COMMISSION OF CYBERCRIME OFFENSES AS DEFINED UNDER THIS ACT SHALL BE DEEMED AN ACT OF ECONOMIC SABOTAGE, WARRANTING THE SEVEREST PENALTIES ALLOWABLE UNDER LAW TO ENSURE DETERRENCE AND ACCOUNTABILITY.

IN PURSUIT OF THIS POLICY, THE STATE SHALL ADOPT AND EXERCISE SUFFICIENT POWERS TO EFFECTIVELY PREVENT, DETECT, INVESTIGATE, AND PROSECUTE CYBERCRIME OFFENSES, WHETHER COMMITTED DOMESTICALLY OR TRANSNATIONALLY, AND SHALL PROVIDE FOR FAST, RELIABLE, AND SECURE MECHANISMS OF INTERNATIONAL COOPERATION, CONSISTENT AT ALL TIMES WITH THE CONSTITUTIONAL SAFEGUARDS OF DUE PROCESS, THE RIGHT TO PRIVACY, AND PROTECTION AGAINST UNREASONABLE SEARCHES AND SEIZURES.

Section 3. Definition of Terms. – For purposes of this Act, the following terms are hereby defined as follows:

- (a) *Access* refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network
- (b) *Alteration* refers to the modification or change, in form or substance, of an existing computer data or program.
- (c) *Communication* refers to the transmission of information through ICT media, including voice, video and other forms of data.
- (d) *Computer* refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device

including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.

(e) *Computer data* refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer systems or online.

(f) *Computer program* refers to a set of instructions executed by the computer to achieve intended results.

(g) *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.

(h) *CRITICAL INFRASTRUCTURE* SHALL REFER TO AN ASSET OR SYSTEM, WHETHER PHYSICAL OR VIRTUAL, SO ESSENTIAL TO THE MAINTENANCE OF VITAL SOCIETAL FUNCTIONS OR TO THE DELIVERY OF ESSENTIAL PUBLIC SERVICES THAT THE INCAPACITY OR DESTRUCTION OF SUCH SYSTEMS AND ASSETS WOULD HAVE A DEBILITATING IMPACT ON NATIONAL DEFENSE AND SECURITY, NATIONAL ECONOMY, PUBLIC HEALTH OR SAFETY, THERE ADMINISTRATION OF JUSTICE, AND OTHER FUNCTIONS ANALOGOUS THERETO. IT MAY INCLUDE, BUT IS NOT LIMITED TO, AN ASSET OR SYSTEM AFFECTING TELECOMMUNICATIONS, WATER AND ENERGY SUPPLY, EMERGENCY SERVICES, FOOD SECURITY, FUEL SUPPLY, BANKING AND FINANCE, TRANSPORTATION, RADIO AND TELEVISION, INFORMATION SYSTEMS AND TECHNOLOGY, CHEMICAL AND NUCLEAR SECTORS.

(i) *Cyber* refers to a computer or a computer network, the electronic medium in which online communication takes place.

(j) *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.

(k) *Database* refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system.

(l) *IDENTIFYING INFORMATION* REFERS TO ANY NAME OR NUMBER THAT MAY BE USED ALONE OR IN CONJUNCTION WITH ANY OTHER INFORMATION TO IDENTIFY ANY SPECIFIC INDIVIDUAL, INCLUDING ANY OF THE FOLLOWING:

(1) NAME, DATE OF BIRTH, DRIVER'S LICENSE NUMBER, PASSPORT NUMBER, TAX IDENTIFICATION NUMBER, OR OTHER GOVERNMENT - ISSUED IDENTIFICATION NUMBER;

(2) UNIQUE BIOMETRIC DATA, SUCH AS FINGERPRINT OR OTHER UNIQUE PHYSICAL REPRESENTATION;

(3) UNIQUE ELECTRONIC IDENTIFICATION NUMBER, ADDRESS, OR ROUTING CODE; AND

(4) TELECOMMUNICATION IDENTIFYING INFORMATION OR ACCESS DEVICES.

(m) *Interception* refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.

(n) *INTERNET INTERMEDIARIES* REFER TO PERSONS OR ENTITIES THAT PROVIDE INFRASTRUCTURE, PLATFORMS, ACCESS TO, AND HOST, TRANSMIT, AND INDEX CONTENT, PRODUCTS, AND SERVICES ORIGINATED BY THIRD PARTIES ON THE INTERNET. THESE INCLUDE, AMONG OTHERS:

- (1) INTERNET SERVICE PROVIDERS;
- (2) WEB HOSTING PROVIDERS INCLUDING DOMAIN NAME REGISTRARS;
- (3) INTERNET SEARCH ENGINES AND PORTALS;
- (4) E -COMMERCE INTERMEDIARIES;
- (5) INTERNET PAYMENT SYSTEM PROVIDERS; AND
- (6) PARTICIPATIVE NETWORK PLATFORM PROVIDERS INCLUDING SOCIAL MEDIA INTERMEDIARIES.

(o) *INTERNET SERVICE PROVIDER (ISP)* REFERS TO A PUBLIC TELECOMMUNICATION ENTITY (PTE) OR VALUE -ADDED SERVICE (VAS) PROVIDER DULY AUTHORIZED BY OR REGISTERED WITH THE NATIONAL TELECOMMUNICATIONS COMMISSION (NTC) THAT PROVIDES USERS OR OTHER ENTITIES WITH DATA CONNECTION ALLOWING ACCESS TO THE INTERNET THROUGH PHYSICAL TRANSPORT INFRASTRUCTURE OR SATELLITE INTERNET PROVIDERS, AND SUCH ACCESS IS NECESSARY FOR INTERNET USERS TO ACCESS CONTENT AND SERVICES ON THE INTERNET, AND FOR CONTENT PROVIDERS TO PUBLISH OR DISTRIBUTE MATERIALS ONLINE.

(p) *MASS MAILER* REFERS TO A SERVICE OR SOFTWARE USED TO SEND ELECTRONIC COMMUNICATIONS TO AN AGGREGATE OF FIFTY (50) OR MORE RECIPIENTS.

(q) *ORGANIZED CRIME GROUP* SHALL MEAN A STRUCTURED GROUP OF THREE (3) OR MORE PERSONS, ACTING IN CONCERT WITH THE AIM OF COMMITTING ONE OR MORE SERIOUS CRIMES OR OFFENSES, IN

ORDER TO OBTAIN, DIRECTLY OR INDIRECTLY, A FINANCIAL OR OTHER MATERIAL BENEFIT.

(r) *OVER-THE-TOP (OTT)* APPLICATIONS REFER TO DIGITAL SERVICES DELIVERED OVER THE INTERNET THAT PROVIDE COMMUNICATION, CONTENT, OR FUNCTIONAL SERVICES TRADITIONALLY OFFERED BY TELECOMMUNICATIONS OR MEDIA PROVIDERS, WITHOUT OWNING OR DIRECTLY CONTROLLING THE UNDERLYING NETWORK INFRASTRUCTURE.

OTT APPLICATIONS INCLUDE SERVICES FOR MESSAGING, VOICE, OR VIDEO COMMUNICATION; CONTENT DELIVERY OR STREAMING; DIGITAL MARKETPLACES OR PLATFORM-BASED SERVICES; FINANCIAL OR TRANSACTIONAL FACILITATION CONDUCTED OVER THE INTERNET.

(s) Service provider refers to:

(1) Any public or private entity that provides to users of its service the ability to communicate by means of a computer system;

(2) Any other entity that processes or stores computer data on behalf of such communication service or users of such service;

(3) ANY ENTITY CONTRACTED BY ANOTHER ENTITY, WHETHER DOMESTIC OR FOREIGN, TO PROCESS ANY DATA OR INFORMATION OF ANY PERSON WHEREVER LOCATED, INCLUDING ENTITIES PROVIDING BUSINESS PROCESS OUTSOURCING AND SIMILAR SERVICES;

(4) PAYMENT SYSTEM PROVIDER (PSP) OR AN ENTITY ENGAGED IN ANY MONETARY TRANSACTION, WHICH INCLUDES BANKS, FIAT OR DIGITAL MONEY SERVICE BUSINESSES INCLUDING CRYPTOCURRENCIES, CREDIT CARD COMPANIES, AND OTHER FINANCIAL INSTITUTIONS; AND

(5) INTERNET INTERMEDIARIES AND INTERNET SERVICE PROVIDER AS DEFINED IN THIS ACT.

(t) *SOCIAL ENGINEERING SCHEME* IS COMMITTED BY A PERSON WHO OBTAINS SENSITIVE IDENTIFYING INFORMATION OF ANOTHER PERSON, THROUGH DECEPTION OR FRAUD, RESULTING IN UNAUTHORIZED ACCESS AND CONTROL OVER THE PERSON'S FINANCIAL ACCOUNT, BY PERFORMING ANY OF THE FOLLOWING ACTS:

- (1) MISREPRESENTING ONESELF AS ACTING ON BEHALF OF AN INSTITUTION, OR MAKING FALSE REPRESENTATIONS TO SOLICIT ANOTHER PERSON'S SENSITIVE IDENTIFYING INFORMATION; OR
- (2) USING ELECTRONIC COMMUNICATIONS TO OBTAIN ANOTHER PERSON'S SENSITIVE IDENTIFYING INFORMATION.

(u) *SOCIAL MEDIA* PLATFORMS REFER TO ONLINE SERVICES OR PLATFORMS THAT ENABLE USERS TO CREATE, UPLOAD, SHARE, DISSEMINATE, OR INTERACT WITH CONTENT OR OTHER USERS, INCLUDING THROUGH TEXT, IMAGES, AUDIO, VIDEO, OR LIVE STREAMING, AND THAT FACILITATE PUBLIC OR SEMI-PUBLIC COMMUNICATION, NETWORKING, OR COMMUNITY FORMATION.

(v) Subscriber's information refers to any information contained in the form of computer data or any other form that is held OR ACCESSED by a service provider, relating to subscribers, WHO MAY BE LOCATED IN THE PHILIPPINES OR NOT, of its services other than traffic or content data and by which identity can be established:

- (1) The type of communication service used, the technical provisions taken thereto and the period of service;
- (2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and

- (3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
- (w) *Traffic data* or non-content data refers to any computer data other than the content of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service.
- (x) *Without right* refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law.

CHAPTER II

PUNISHABLE ACTS

Section 4. Cybercrime Offenses. – The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity, availability, NON-REPUDIATION, AUTHENTICATION, PRIVACY, AND SAFETY of computer data and systems:

(1) **Illegal Access.** – The access to the whole or any part of AN ICT system without right. ILLEGAL ACCESS SHALL INCLUDE THE INFRINGEMENT OF SECURITY MEASURES WITH THE INTENT OF OBTAINING ELECTRONIC DATA WITHOUT RIGHT FROM THE OWNER OR OTHER DISHONEST OR CRIMINAL INTENT OR IN RELATION TO AN ICT SYSTEM THAT IS CONNECTED TO ANOTHER ICT SYSTEM.

(2) **Illegal Interception.** – INTENTIONALLY AND WITHOUT RIGHT, the interception, made by technical means, of non-public transmission of ELECTRONIC DATA TO, from or within AN ICT system.

(3) **Data Interference.** — The intentional alteration, INPUTTING, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or

transmission of MALWARE, REGARDLESS OF WHO CONTROLS OR OWNS THE COMPUTER DATA.

(4) System Interference. — The intentional alteration, INTERFERENCE IN WHOLE OR IN PART, of the functioning of a AN ICT TECHNOLOGY SYSTEM by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing without right or authority, including the introduction or transmission of MALWARE TO THE ICT SYSTEM.

(5) Misuse of Devices. —

(i) The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

(aa) A device OR ANY HARDWARE COMPONENT, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or

(bb) A computer password, SYSTEM AND NETWORK CREDENTIALS, access code, APPLICATION, MALWARE or similar data, or ANY HARDWARE COMPONENT by which the whole or any part of a computer system is capable of being accessed with THE intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The MERE possession of an item referred to in paragraphs 5(i)(aa) or (bb) above EITHER USED IN, OR with intent to use said devices for the purpose of committing any of the offenses under this section: PROVIDED, THAT, THERE IS A PRESUMPTION AND PRIMA FACIE EVIDENCE OF INTENT TO USE SAID DEVICES BY MERE POSSESSION, CONTROL, OR CUSTODY BY A NATURAL OR JURIDICAL PERSON WHOSE BUSINESS OR EMPLOYMENT DOES NOT LAWFULLY DEAL WITH THE USE, PRODUCTION, MANUFACTURE, PROCUREMENT, IMPORTATION, OR DISTRIBUTION THEREOF, OR NOT IN THE ORDINARY COURSE OF THE POSSESSOR'S TRADE OR BUSINESS.

(6) Cyber-squatting. – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, OR deprive others from registering the same, if such a domain name is:

- (i) Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
- (ii) Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
- (iii) Acquired without right or with intellectual property interests in it.

(7) MALICIOUS REFUSAL TO SURRENDER COMPUTER DATA OR COMPUTER SYSTEM. – ANY PERSON WHO MALICIOUSLY AND UNLAWFULLY POSSESSES, RETAINS OR REFUSES TO SURRENDER ANY COMPUTER OR COMPUTER SYSTEM THAT CONTAINS DATA IN THE FORM OF PERSONAL INFORMATION, SENSITIVE PERSONAL INFORMATION, OR PRIVILEGED INFORMATION UNDER RA 10173 OR THE "DATA PRIVACY ACT OF 2012," TO THE LAWFUL OR RIGHTFUL OWNER OR POSSESSOR OF THE COMPUTER OR COMPUTER SYSTEM OR PROCESSOR OF SUCH DATA.

(b) Computer-related Offenses:

(1) Computer-related Forgery. —

- (i) The input, alteration, deletion OR SUPPRESSION, of any ELECTRONIC data, without right, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or

(ii) The act of knowingly using ELECTRONIC data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

(2) Computer-related Fraud. —

(a) The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing ANY FORM OF damage, WHETHER DIRECT OR INDIRECT, thereby with fraudulent intent: Provided, that, if no damage has been caused, the penalty imposable shall be one (1) degree lower;

(b) ANY DECEPTION AS TO FACTUAL CIRCUMSTANCES MADE THROUGH AN ICT SYSTEM THAT CAUSES A PERSON TO DO OR OMIT TO DO ANYTHING WHICH THAT PERSON WOULD NOT OTHERWISE DO OR OMIT TO DO;

(c) THE COMMISSION OF ARTICLES 315, 316, 317 AND 318 OF THE REVISED PENAL CODE THROUGH THE USE OF ICT SYSTEM.

(3) Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: Provided, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(c) Content-related Offenses:

(1) CYBERSEX AS A MEANS OF SCAM OR FRAUDULENT OPERATION. — THE USE OF SEXUALLY EXPLICIT, SUGGESTIVE, OR INTIMATE ACTS, REPRESENTATIONS, COMMUNICATIONS, OR INTERACTIONS, WHETHER REAL OR SIMULATED, INCLUDING LIVE OR RECORDED PERFORMANCES, INTERACTIVE MESSAGING, OR DIGITALLY GENERATED CONTENT, THROUGH A COMPUTER SYSTEM, SOCIAL MEDIA PLATFORM, OR ANY ONLINE SERVICE,

FOR THE PURPOSE OF DECEIVING, MANIPULATING, COERCING, OR INDUCING ANOTHER PERSON TO PART WITH MONEY, PROPERTY, DIGITAL ASSETS, OR ANY BENEFIT, OR TO FACILITATE, CONCEAL, OR ADVANCE A SCAM, FRAUDULENT SCHEME, OR ORGANIZED CYBERCRIME OPERATION.

SUCH OFFENSE SHALL BE COMMITTED REGARDLESS OF WHETHER ACTUAL SEXUAL ACTIVITY OCCURRED, OR WHETHER THE VICTIM PERSONALLY TESTIFIES, WHERE INTENT TO DEFRAUD OR EXPLOIT MAY BE ESTABLISHED THROUGH DIGITAL EVIDENCE, FINANCIAL RECORDS, COMMUNICATIONS, PLATFORM DATA, OR OTHER COMPETENT PROOF OBTAINED DURING LAWFUL INVESTIGATION.

ANY PERSON WHO KNOWINGLY ORGANIZES, MANAGES, FINANCES, MAINTAINS, OR PROVIDES FACILITIES OR DIGITAL INFRASTRUCTURE FOR THE COMMISSION OF CYBERSEX-RELATED SCAM OPERATIONS SHALL BE LIABLE AS A PRINCIPAL OR ACCOMPLICE UNDER THIS ACT.

(2) Libel. — The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

Section 5. Other Offenses. — The following acts shall also constitute an offense:

(a) Aiding or Abetting in the Commission of Cybercrime. — Any person who willfully abets or aids in the commission of, OR INFLUENCES OR DECEIVES ANOTHER TO COMMIT any of the offenses enumerated in this Act shall be held liable.

(b) Attempt in the Commission of Cybercrime. — Any person who willfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

(c) SOLICITATION TO COMMIT CYBERCRIME. – ANY PERSON WHO WILFULLY PROPOSES, SOLICITS, OR INDUCES ANOTHER PERSON TO COMMIT ANY OF THE OFFENSES UNDER THIS ACT, SHALL BE HELD LIABLE.

SECTION 6. USE OF ICT FOR ALL OTHER CRIMES AND IMPOSABLE PENALTY. – ALL CRIMES, NOT MENTIONED ABOVE, DEFINED AND PENALIZED BY THE REVISED PENAL CODE, AS AMENDED, AND SPECIAL LAWS, IF COMMITTED BY, THROUGH AND WITH THE USE OF ICTS SHALL BE COVERED BY THE RELEVANT PROVISIONS OF THIS ACT: PROVIDED, THAT THE PENALTY TO BE IMPOSED SHALL BE ONE (1) DEGREE HIGHER THAN THAT PROVIDED FOR BY THE REVISED PENAL CODE, AS AMENDED, AND SPECIAL LAWS, AS THE CASE MAY BE: PROVIDED, FURTHER, THAT THE PROSECUTION OF THE OFFENSES UNDER THIS ACT MAY BE INITIATED BY ANY OFFENDED PARTY OR ANY AFFECTED SERVICE PROVIDER.

SECTION 7. CYBERCRIMES CONSTITUTING ECONOMIC SABOTAGE. – ANY PERSON WHO COMMITS CYBERCRIME WHEN SUCH ACTS RESULT IN SERIOUS ECONOMIC HARM EXCEEDING ONE HUNDRED MILLION PESOS (PHP 100,000,000.00) OR WHEN THEY TARGET OR DISRUPT CRITICAL INFRASTRUCTURE SHALL BE DEEMED TO HAVE COMMITTED AN ACT OF ECONOMIC SABOTAGE.

ECONOMIC SABOTAGE SHALL ALSO BE APPRECIATED IF THE CYBERCRIME IS COMMITTED UNDER ANY OF THE FOLLOWING CIRCUMSTANCES:

1. BY A GROUP OF THREE (3) OR MORE PERSONS CONSPIRING OR CONFEDERATING WITH ONE ANOTHER (ORGANIZED CRIME GROUP);
2. AGAINST THREE (3) OR MORE PERSONS, INDIVIDUALLY OR COLLECTIVELY;

3. USING A MASS MAILER, AUTOMATED SERVICE, SOFTWARE, OR ANY OTHER SCALABLE DELIVERY METHOD, INCLUDING SOCIAL ENGINEERING OR SIMILAR FRAUDULENT SCHEMES; OR
4. THROUGH HUMAN TRAFFICKING.

Section 8. 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 III PENALTIES

SECTION 9. PENALTIES. — Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of prision mayor or a fine of at least Two hundred thousand pesos (Php 200,000.00) up to a maximum amount commensurate to the damage incurred, or both.

Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of prision mayor or a fine of not more than Five hundred thousand pesos (Php 500,000.00), or both.

ANY PERSON FOUND GUILTY OF ANY OF THE PUNISHABLE ACTS ENUMERATED IN SECTION 4(C)(1) OF THIS ACT SHALL BE PUNISHED WITH IMPRISONMENT OF PRISON MAYOR OR A FINE OF AT LEAST TWO HUNDRED THOUSAND PESOS (PHP200,000.00) BUT NOT EXCEEDING ONE MILLION PESOS (PHP1,000,000.00) OR BOTH.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act, COMMITTED THROUGH A COMPUTER SYSTEM, shall be punished with the penalty one (1) degree higher than that provided for in the RA 11930, ALSO KNOWN AS THE ANTI-ONLINE SEXUAL ABUSE OR EXPLOITATION OF CHILDREN (OSAEC) AND ANTI-CHILD SEXUAL ABUSE OR EXPLOITATION MATERIALS (CSAEM) ACT.

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (Php 100,000.00) but not exceeding Five hundred thousand pesos (Php 500,000.00) or both.

ACTS OF ECONOMIC SABOTAGE AS SET OUT IN SECTION 7 SHALL BE PUNISHABLE BY LIFE IMPRISONMENT AND A FINE TWICE THE VALUE OR THE TOTAL HARM OR LOSSES INVOLVED, WITHOUT PREJUDICE TO PROSECUTION UNDER OTHER APPLICABLE LAWS.

Section 10. Corporate Liability. — When any of the punishable acts herein defined are committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on: (a) a power of representation of the juridical person provided the act committed falls within the scope of such authority; (b) an authority to take decisions on behalf of the juridical person: Provided, That the act committed falls within the scope of such authority; or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable UP TO A MAXIMUM OF FIFTEEN MILLION PESOS (PHP 15,000,000.00).

If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in SECTION 8 up to a maximum of TEN MILLION PESOS (PHP10,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

CHAPTER IV

STRATEGIC AND COMPREHENSIVE ENFORCEMENT AND IMPLEMENTATION

SECTION 11. NATIONAL CYBERCRIME PREVENTION AND INVESTIGATION AGENCY. – THERE IS HEREBY CREATED A UNIFIED IMPLEMENTATION BODY HEREOF TO BE KNOWN AS THE NATIONAL CYBERCRIME PREVENTION AND INVESTIGATION AGENCY (NCPIA). THE NCPIA SHALL SERVE AS THE PRIMARY GOVERNMENT AGENCY RESPONSIBLE FOR THE EFFICIENT AND EFFECTIVE PREVENTION, DETECTION, INVESTIGATION, AND SUPPRESSION OF ALL FORMS OF CYBERCRIME IN THE PHILIPPINES.

THE NCPIA SHALL EXERCISE THE FOLLOWING POWERS AND FUNCTIONS:

- (A) PROVIDE SECRETARIAT SUPPORT TO THE NATIONAL ANTI-CYBERCRIME COUNCIL (NACC);
- (B) IMPLEMENT, OR CAUSE THE EFFECTIVE IMPLEMENTATION OF, THE NATIONAL CYBERCRIME PREVENTION STRATEGY (NCPS) AND RELATED POLICIES, BY INSTITUTIONALIZING THE USE OF APPROPRIATE DIGITAL TOOLS, PLATFORMS, AND TECHNOLOGICAL SOLUTIONS TO ENHANCE OPERATIONAL EFFICIENCY, MONITORING, AND ENFORCEMENT OUTCOMES;
- (C) DEVELOP, COORDINATE AND IMPLEMENT A LAW ENFORCEMENT SECTOR-WIDE CAPABILITY BUILDING FRAMEWORK AND PROGRAM THAT INSTITUTIONALIZES THE STRATEGIC USE OF APPROPRIATE TECHNOLOGIES AND INTERNATIONAL BEST PRACTICES TO ENHANCE INVESTIGATIVE, OPERATIONAL, AND ENFORCEMENT CAPACITIES;
- (D) LEAD THE ENFORCEMENT OF THE PROVISIONS OF THIS ACT, AND UNDERTAKE THE INVESTIGATION AND PROSECUTION OF VIOLATORS, AS WELL AS RELATED MATTERS ARISING FROM THE COMMISSION OF PUNISHABLE ACTS HEREIN, IN ACCORDANCE WITH PRIORITIZATION CRITERIA — PARTICULARLY CASES OF NATIONAL SIGNIFICANCE AND THOSE NECESSITATING

COORDINATED ACTION — SET FORTH UNDER THE NCPS OR BY THE NACC: PROVIDED, THAT, THERE IS HEREBY ESTABLISHED AN INTER-AGENCY COMMITTEE ON CYBERCRIME, TO BE COORDINATED BY NCPIA EXECUTIVE DIRECTOR, TO ENSURE THAT LAW ENFORCEMENT AUTHORITIES AND OTHER CONCERNED AGENCIES ALIGN WITH AND IMPLEMENT THE NCPS AND ALL RELEVANT POLICIES FORMULATED BY THE NACC IN AN INTEGRATED AND SYNCHRONIZED MANNER;

(E) ADMINISTER OATHS, AND ISSUE SUBPOENA AND SUBPOENA DUCES TECUM RELATIVE TO INVESTIGATIONS INVOLVING VIOLATIONS OF THIS ACT;

(F) EFFECT THE ARREST, SEARCH, AND SEIZURE OF VIOLATORS, AS WELL AS THE CONFISCATION OF THE PROCEEDS OR INSTRUMENTALITIES OF CYBERCRIME, IN ACCORDANCE WITH LAW, AND FOR THIS PURPOSE, DULY DESIGNATED ENFORCEMENT OFFICERS OF THE NCPIA, UNDER NACC'S POLICIES, ARE AUTHORIZED TO BEAR FIREARMS CONSISTENT WITH EXISTING LAWS;

(G) ESTABLISH AND MANAGE AN INTER-AGENCY ANTI-SCAM HUB THAT WILL STRENGTHEN COORDINATED INVESTIGATIONS OF SCAM- RELATED CRIMES, DISRUPT ILLICIT OPERATIONS, AND ASSIST IN RECOVERY AND MITIGATING VICTIMS' LOSSES, IN COLLABORATION WITH STAKEHOLDERS;

(H) ESTABLISH AND OPERATE DIGITAL FORENSIC LABORATORIES TO EXAMINE SEIZED OR CONFISCATED CYBERCRIME-RELATED PROCEEDS, MATERIALS, AND PARAPHERNALIA, AND TO FACILITATE THEIR LAWFUL DISPOSITION;

(I) CLOSELY COORDINATE WITH DICT-CYBERSECURITY BUREAU (CSB), IN FURTHERANCE OF CYBERCRIME PREVENTION, TO CONTINUOUSLY UPDATE AND STRENGTHEN IMPLEMENTATION OF CYBER-RESPONSIBILITY STANDARDS, DIGITAL SECURITY PROTOCOLS, AND RESPONSIBLE ONLINE PRACTICES, DESIGNED TO SAFEGUARD CONSUMERS, STRENGTHEN TRUST IN DIGITAL

ECOSYSTEMS, AND ENABLE EFFICIENT DIGITAL FORENSIC INVESTIGATIONS IN CYBERCRIME CASES;

(J) FOSTER COMMUNITY-BASED PARTICIPATION IN CYBERCRIME PREVENTION AND SUPPRESSION;

(K) ESTABLISH AND SUSTAIN CLOSE COORDINATION AND LINKAGES WITH INTERNATIONAL CYBERCRIME AGENCIES AND ORGANIZATIONS, AND RELEVANT BILATERAL PARTNERS, AND IMPLEMENT THE APPLICABLE PROVISIONS OF INTERNATIONAL CONVENTIONS AND AGREEMENTS TO WHICH THE PHILIPPINES IS A STATE PARTY;

(L) CALL ON THE ASSISTANCE OF ANY DEPARTMENT, BUREAU, OFFICE, AGENCY, INSTRUMENTALITY, OR GOVERNMENT-OWNED OR - CONTROLLED CORPORATION (GOCC) IN THE ANTI-CYBERCRIME DRIVE, INCLUDING THE MOBILIZATION OF THEIR PERSONNEL, FACILITIES, AND RESOURCES, TO STRENGTHEN THE DETECTION, INVESTIGATION, AND PROSECUTION OF CYBERCRIME.

SECTION 12. ORGANIZATIONAL AND COMPOSITION OF NCPIA. – THE NCPIA SHALL BE HEADED BY THE DIRECTOR GENERAL WHO SHALL BE RESPONSIBLE FOR THE GENERAL ADMINISTRATION AND MANAGEMENT THEREOF. HE/SHE SHALL BE ASSISTED BY TWO (2) DEPUTY DIRECTORS GENERAL.

TO EFFECTIVELY FULFILL ITS MANDATE IN ADDRESSING THE COMPLEX AND RAPIDLY EVOLVING LANDSCAPE OF CYBERCRIME, THE NCPIA SHALL BE COMPOSED OF SPECIALIZED SERVICES AND OFFICES, HEADED BY DIRECTORS IV AND, ASSISTED BY DIRECTORS III, INCLUDING BUT NOT LIMITED TO THE FOLLOWING:

1. DIRECTORATE FOR INVESTIGATION – RESPONSIBLE FOR THE CONDUCT OF CYBERCRIME INVESTIGATIONS, CASE BUILD-UP, AND COORDINATION WITH LAW ENFORCEMENT, BOTH

LOCAL AND INTERNATIONAL, AND PROSECUTORIAL AGENCIES, AS WELL AS CYBER INTELLIGENCE GATHERING AND ANALYSIS.

2. DIRECTORATE FOR LEGAL AFFAIRS – PROVIDES LEGAL ADVICE, ASSISTS IN THE PROSECUTION OF CASES, DRAFTS CONTRACTS AND AGREEMENTS, AND ENSURES COMPLIANCE WITH NATIONAL AND INTERNATIONAL LEGAL FRAMEWORKS.

3. DIRECTORATE FOR POLICY, PLANNING AND COORDINATION – DEVELOPS POLICIES, STRATEGIC PLANS, AND PROGRAMS ALIGNED WITH THE NATIONAL CYBERCRIME PREVENTION STRATEGY AND INTERNATIONAL BEST PRACTICES, LEVERAGES DATA ANALYTICS TO GENERATE EVIDENCE-BASED POLICY RECOMMENDATIONS, STRENGTHENS PARTNERSHIPS WITH FOREIGN COUNTERPARTS, REGIONAL BODIES, AND INTERNATIONAL ORGANIZATIONS, AND MONITORS IMPLEMENTATION OUTCOMES.

4. DIRECTORATE FOR DIGITAL FORENSICS, TECHNOLOGY AND INNOVATION – SERVES AS THE AGENCY’S TECHNICAL AUTHORITY ON DIGITAL EVIDENCE AND CYBERCRIME INVESTIGATIVE CAPABILITIES; OPERATES AND MAINTAINS DIGITAL FORENSIC LABORATORIES; CONDUCTS THE ACQUISITION, PRESERVATION, EXAMINATION, ANALYSIS, AND REPORTING OF DIGITAL EVIDENCE IN ACCORDANCE WITH INTERNATIONALLY ACCEPTED FORENSIC STANDARDS TO ENSURE ADMISSIBILITY IN JUDICIAL AND QUASI-JUDICIAL PROCEEDINGS; AND DEVELOPS, VALIDATES, AND OPERATIONALLY APPLIES SPECIALIZED CYBERCRIME INVESTIGATION TOOLS, FORENSIC METHODOLOGIES, AND INNOVATIVE TECHNICAL SOLUTIONS FOR INVESTIGATIVE, INTELLIGENCE, AND EVIDENTIARY PURPOSES, WITHOUT EXERCISING ENTERPRISE INFORMATION SYSTEMS MANAGEMENT, GENERAL INFORMATION TECHNOLOGY

ADMINISTRATION, OR AGENCY-WIDE INFRASTRUCTURE SUPPORT FUNCTIONS.

5. DIRECTORATE FOR TRAINING – DESIGNS, DEVELOPS, AND DELIVERS, IN COORDINATION WITH AND LEVERAGING EXISTING GOVERNMENT ACADEMIES OR TRAINING INSTITUTIONS AND FACILITIES, STANDARDIZED, COMPETENCY-BASED TRAINING PROGRAMS TO STRENGTHEN THE CYBERCRIME PREVENTION, INVESTIGATION, PROSECUTION, AND DIGITAL FORENSICS CAPABILITIES OF LAW ENFORCEMENT, PROSECUTORS, REGULATORS, AND OTHER AUTHORIZED STAKEHOLDERS, ENSURING THAT TRAINING CURRICULA ARE ALIGNED WITH THE NCPS, RELEVANT LAWS AND POLICIES, EMERGING TECHNOLOGICAL TRENDS, AND INTERNATIONAL BEST PRACTICES, AND ARE INFORMED BY OPERATIONAL REALITIES AND EVOLVING CYBER THREATS: PROVIDED, THAT, THE TRAINING DIRECTORATE SHALL INSTITUTIONALIZE CONTINUOUS PROFESSIONAL DEVELOPMENT THROUGH MODULAR COURSES, SIMULATIONS, CERTIFICATIONS, AND INTER-AGENCY TRAINING INITIATIVES, WHILE FOSTERING PARTNERSHIPS WITH LOCAL AND INTERNATIONAL INSTITUTIONS TO ENHANCE TECHNICAL EXPERTISE, OPERATIONAL READINESS, AND INTER-OPERABILITY ACROSS THE NATIONAL CYBERCRIME RESPONSE ECOSYSTEM.

6. DIRECTORATE FOR HUMAN RESOURCE AND ADMINISTRATION – MANAGES PERSONNEL RECRUITMENT, TRAINING, AND CAPACITY- BUILDING PROGRAMS FOR NCPIA, AS WELL AS ADMINISTRATIVE SUPPORT FOR EFFICIENT AGENCY OPERATIONS.

THE DG AND TWO (2) DDGs SHALL BE APPOINTED BY THE PRESIDENT AND SHALL HAVE THE RANK, SALARY AND BENEFITS EQUIVALENT TO THAT OF AN UNDERSECRETARY AND ASSISTANT SECRETARY, RESPECTIVELY. NO PERSON SHALL BE APPOINTED DG OR DDG UNLESS HE OR SHE IS A NATURAL BORN CITIZEN OF THE PHILIPPINES, AT LEAST THIRTY-FIVE (35) YEARS OF AGE ON THE DAY OF THEIR APPOINTMENT,

OF PROVEN COMPETENCE, INTEGRITY, PROBITY AND INDEPENDENCE, AND POSSESSES TEN (10) YEARS OF EXPERIENCE OR PROFESSIONAL PRACTICE FOR THE DG, AND SEVEN (7) YEARS OF EXPERIENCE OR PROFESSIONAL PRACTICE FOR THE DDG, IN THE FIELDS OF ICT, CYBERCRIME INVESTIGATION, CYBERSECURITY, LAW ENFORCEMENT, OR LAW. THE DIRECTORS SHALL ALSO HAVE THE SAME QUALIFICATIONS EXCEPT THAT THEY SHALL BE AT LEAST TWENTY FIVE (25) YEARS OF AGE, AND HAVE AT LEAST FIVE (5) YEARS OF EXPERIENCE OR PRACTICE IN THE ABOVE FIELDS.

THERE SHALL ALSO BE CREATED THE OFFICE OF THE CHIEF INFORMATION AND TECHNOLOGY OFFICER (OCITO) AND THE OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER (OCISO), REPORTING TO THE DG, THUS:

1. OCITO, HEADED BY A CHIEF INFORMATION AND TECHNOLOGY OFFICER, WHICH SHALL BE RESPONSIBLE FOR ENTERPRISE INFORMATION SYSTEMS, TECHNOLOGY ARCHITECTURE, DATA AND SYSTEMS INTEGRATION, CYBERSECURITY GOVERNANCE IN COORDINATION WITH THE CHIEF INFORMATION SECURITY OFFICER, AND THE DELIVERY, MAINTENANCE, AND RELIABILITY OF MISSION- CRITICAL IT SERVICES OF THE AGENCY; THE OCITO SHALL EXERCISE FUNCTIONAL SUPERVISION OVER ALL MIS AND IT SUPPORT UNITS AND SHALL COORDINATE WITH ALL DIRECTORATES, INCLUDING THE DIRECTORATE FOR DIGITAL FORENSICS, TECHNOLOGY AND INNOVATION, TO ENSURE THAT ENTERPRISE SYSTEMS SUPPORT OPERATIONAL REQUIREMENTS WHILE PRESERVING FORENSIC INTEGRITY, WITHOUT DIRECTING OR CONTROLLING FORENSIC EXAMINATIONS, EVIDENTIARY ANALYSIS, OR INVESTIGATIVE METHODOLOGIES; AND

2. OCISO, HEADED BY A CHIEF INFORMATION SECURITY OFFICER (CISO), WHICH SHALL SERVE AS THE CENTRAL

AUTHORITY FOR INFORMATION SECURITY GOVERNANCE OF THE AGENCY AND SHALL BE RESPONSIBLE FOR THE DEVELOPMENT, IMPLEMENTATION, AND ENFORCEMENT OF ENTERPRISE CYBERSECURITY AND INFORMATION SECURITY POLICIES, STANDARDS, AND CONTROLS; THE PROTECTION OF SENSITIVE INVESTIGATIVE, FORENSIC, OPERATIONAL, AND ADMINISTRATIVE INFORMATION AND SYSTEMS; CYBERSECURITY RISK MANAGEMENT, MONITORING, AND INCIDENT RESPONSE; AND COORDINATION WITH THE OCITO AND ALL DIRECTORATES TO ENSURE SECURITY-BY-DESIGN ACROSS AGENCY SYSTEMS, WITHOUT INTERFERING WITH THE SUBSTANTIVE CONDUCT OF INVESTIGATIONS OR FORENSIC EXAMINATIONS.

THE NCPIA SHALL ALSO ENSURE THAT A DATA PRIVACY OFFICER, IN ACCORDANCE WITH APPLICABLE LAWS AND REGULATIONS, IS APPOINTED.

SECTION 13. NATIONAL ANTI-CYBERCRIME COUNCIL. – TO ENSURE A WHOLE-OF-GOVERNMENT APPROACH AND COMPREHENSIVE POLICY DIRECTION, A GOVERNING BODY FOR THE NCPIA KNOWN AS THE NATIONAL ANTI-CYBERCRIME COUNCIL (NACC), IS HEREBY CREATED. THE NACC SHALL SERVE AS THE PRINCIPAL POLICY-MAKING AND COORDINATING BODY ON MATTERS RELATING TO THE PREVENTION, SUPPRESSION, AND PROSECUTION OF CYBERCRIME, WITH POWERS AND RESPONSIBILITIES SET OUT IN SECTION 14 HEREOF.

THE NACC SHALL BE CHAIRED BY THE SECRETARY OF THE DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT), WITH THE DG OF THE NCPIA SERVING AS VICE-CHAIRPERSON.

THE COUNCIL SHALL BE COMPOSED OF THE FOLLOWING EX OFFICIO MEMBERS, DRAWN FROM THE SENIOR LEVELS OF RELEVANT GOVERNMENT AGENCIES TO ENSURE A MULTIDISCIPLINARY AND

WHOLE-OF-NATION APPROACH TO CYBERCRIME PREVENTION AND INVESTIGATION:

1. CHIEF OF THE PHILIPPINE NATIONAL POLICE (PNP);
2. DIRECTOR OF THE NATIONAL BUREAU OF INVESTIGATION (NBI);
3. COMMISSIONER OF THE NATIONAL TELECOMMUNICATIONS COMMISSION (NTC);
4. SUPERVISING OFFICIAL OR HEAD OF THE CONSUMER ACCOUNT PROTECTION OFFICE (CAPO), BANGKO SENTRAL NG PILIPINAS (BSP), UPON CONCURRENCE OF THE MONETARY BOARD;
5. SUPERVISING OFFICIAL OR HEAD OF THE E-COMMERCE BUREAU, DEPARTMENT OF TRADE AND INDUSTRY (DTI);
6. EXECUTIVE DIRECTOR OF THE DOJ-OFFICE ON CYBERCRIME;
7. EXECUTIVE DIRECTOR OF THE ANTI-MONEY LAUNDERING COUNCIL (AMLC);
8. EXECUTIVE DIRECTOR OF THE PRESIDENTIAL ANTI-ORGANIZED CRIME COMMISSION (PAOCC);
9. EXECUTIVE DIRECTOR OF THE PHILIPPINE CENTER ON TRANSNATIONAL CRIME (PCTC);
10. UNDERSECRETARY FOR CYBERSECURITY OR DIRECTOR, CYBERSECURITY BUREAU – DICT (CSB-DICT), AS THE DICT SECRETARY MAY ASSIGN;
11. COMMANDER OF THE ARMED FORCES OF THE PHILIPPINES (AFP) – CYBERCOMMAND;
12. DIRECTOR-GENERAL OF THE NATIONAL INTELLIGENCE COORDINATING AGENCY (NICA); AND
13. UNDERSECRETARY OF FOREIGN AFFAIRS IN CHARGE OF TRANSNATIONAL CRIME, OR CYBER DIPLOMACY AND CYBER SECURITY, OR THE UNITED NATIONS AND OTHER INTERNATIONAL ORGANIZATIONS, AS THE FOREIGN AFFAIRS SECRETARY MAY ASSIGN.

THE COUNCIL MAY LIKEWISE INVITE AS RESOURCE PERSONS RELEVANT REGULATORS AND REPRESENTATIVES OR EXPERTS FROM THE PRIVATE SECTOR, INCLUDING BUT NOT LIMITED TO THE TELECOMMUNICATIONS, INFORMATION TECHNOLOGY AND BUSINESS PROCESS OUTSOURCING (IT- BPO) INDUSTRIES, FINANCIAL SERVICES, TECHNOLOGY PLATFORMS, AND THE CYBERSECURITY SECTOR, AS WELL AS THE ACADEME AND CIVIL SOCIETY ORGANIZATIONS, IN ORDER TO ENSURE THAT POLICY FORMULATION IS EVIDENCE-BASED, INFORMED BY OPERATIONAL REALITIES, SECTORAL EXPERTISE, EVOLVING TECHNOLOGIES, AND GLOBAL STANDARDS.

SECTION 14. POWERS AND RESPONSIBILITIES OF THE NACC. – THE NACC SHALL BE THE PRINCIPAL POLICY-MAKING, OVERSIGHT, AND COORDINATING BODY ON MATTERS RELATING TO THE PREVENTION, SUPPRESSION, AND PROSECUTION OF CYBERCRIME. TO THIS END, THE NACC SHALL EXERCISE THE FOLLOWING POWERS AND RESPONSIBILITIES:

- (A) FORMULATE, ADOPT, AND PERIODICALLY UPDATE THE NATIONAL CYBERCRIME PREVENTION STRATEGY (NCPS), SETTING FORTH THE LONG-TERM POLICY DIRECTIONS, NATIONAL PRIORITIES, AND INSTITUTIONAL FRAMEWORKS FOR CYBERCRIME PREVENTION AND SUPPRESSION, AND ENSURING THAT THE ENFORCEMENT ACTIONS OF THE NCPIA AND OTHER LAW ENFORCEMENT AUTHORITIES ARE FULLY ALIGNED WITH THE BROADER OBJECTIVES OF NATIONAL SECURITY, ECONOMIC STABILITY, TECHNOLOGICAL INNOVATION, AND PUBLIC TRUST;
- (B) EXERCISE POLICY OVERSIGHT OVER THE NCPIA TO ENSURE THAT ITS OPERATIONS, PROGRAMS, AND ACTIVITIES ARE CONSISTENT WITH THE NCPS AND OTHER POLICIES ADOPTED BY THE COUNCIL;

(C) ESTABLISH AND INSTITUTIONALIZE FORMAL INTER-AGENCY COORDINATION MECHANISMS, THROUGH THE NCPIA ACTING AS ITS SECRETARIAT, TO:

- (1) RESOLVE JURISDICTIONAL AND OPERATIONAL ISSUES AMONG GOVERNMENT AGENCIES;
- (2) AVOID DUPLICATION AND FRAGMENTATION OF MANDATES; AND
- (3) ENSURE THE SYNCHRONIZATION AND INTEGRATION OF ALL GOVERNMENT ACTIONS AGAINST CYBERCRIME;

(D) ISSUE POLICY DIRECTIVES, GUIDELINES, AND STANDARDS BINDING UPON THE NCPIA AND RECOMMEND, WHERE NECESSARY, THE ISSUANCE OF EXECUTIVE OR ADMINISTRATIVE MEASURES TO STRENGTHEN CYBERCRIME PREVENTION, INVESTIGATION, AND ENFORCEMENT;

(E) REVIEW AND EVALUATE THE PERFORMANCE OF THE NCPIA, AND REQUIRE FROM THE LATTER PERIODIC REPORTS ON ITS OPERATIONS, ACCOMPLISHMENTS, AND COMPLIANCE WITH THE NCPS AND OTHER COUNCIL POLICIES;

(F) PROMOTE AND FOSTER COOPERATION AND PARTNERSHIPS WITH THE PRIVATE SECTOR, ACADEME, CIVIL SOCIETY, PROFESSIONAL ASSOCIATIONS, AND THE CITIZENRY TO ENSURE THAT NATIONAL POLICIES ARE INFORMED BY INDUSTRY EXPERTISE, TECHNOLOGICAL TRENDS, AND GLOBAL BEST PRACTICES;

(G) STRENGTHEN LINKAGES AND REPRESENTATION WITH REGIONAL AND INTERNATIONAL ORGANIZATIONS, AND ENSURE THE EFFECTIVE IMPLEMENTATION OF TREATIES, CONVENTIONS, AND OTHER INTERNATIONAL COMMITMENTS ON CYBERCRIME TO WHICH THE PHILIPPINES IS A STATE PARTY;

(H) MOBILIZE GOVERNMENT RESOURCES BY DIRECTING, WHERE APPROPRIATE, DEPARTMENTS, BUREAUS, OFFICES, AGENCIES, OR INSTRUMENTALITIES OF THE GOVERNMENT,

INCLUDING GOVERNMENT-OWNED OR -CONTROLLED CORPORATIONS (GOCCS), TO RENDER SUCH ASSISTANCE, FACILITIES, OR SERVICES AS MAY BE NECESSARY FOR THE EFFECTIVE DISCHARGE OF THE COUNCIL'S FUNCTIONS; AND

(I) PERFORM SUCH OTHER POLICY-MAKING, COORDINATING, AND OVERSIGHT FUNCTIONS AS MAY BE NECESSARY TO CARRY OUT THE INTENT OF THIS ACT.

Section 15 . ROLE OF LAW ENFORCEMENT AGENCIES. — THE CYBERCRIME UNITS OF THE NATIONAL BUREAU OF INVESTIGATION (NBI) AND THE PHILIPPINE NATIONAL POLICE (PNP) SHALL CONTINUE TO PERFORM THEIR FUNCTIONS IN COMBATTING CYBERCRIME: PROVIDED, THAT, THEY SHALL BE ALIGNED WITH THE OBJECTIVES AND THE STRUCTURE ESTABLISHED HEREOF AND THE NCPS TO BE FORMULATED UNDER THE RESPONSIBILITY AND OVERSIGHT OF THE NACC. ALL CYBER INVESTIGATION AND ASSESSMENT CENTERS ESTABLISHED OR PROPOSED TO BE ESTABLISHED BY LAW ENFORCEMENT AUTHORITIES SHALL CONFORM TO THE STANDARDS AND PROTOCOLS TO BE PRESCRIBED BY THE NACC THROUGH THE NCPIA.

Section 16. GRANT OF SUBPOENA POWERS TO THE HEAD, ANTI-CYBERCRIME UNIT OF PNP. — THE HEAD OF PNP ANTI-CYBERCRIME GROUP SHALL HAVE THE POWER TO ADMINISTER OATH, AND ISSUE SUBPOENA AND SUBPOENA DUCES TECUM IN RELATION TO ITS INVESTIGATION. THE SUBPOENA SHALL STATE THE NATURE AND PURPOSE OF INVESTIGATION, SHALL BE DIRECTED TO THE PERSON OR SERVICE PROVIDER WHOSE ATTENDANCE IS REQUIRED, AND IN THE CASE OF A SUBPOENA DUCES TECUM, IT SHALL ALSO CONTAIN A REASONABLE DESCRIPTION OF THE BOOKS, DOCUMENTS, THINGS, DATA OR INFORMATION, DEMANDED WHICH MUST BE RELEVANT TO THE INVESTIGATION.

FAILURE TO COMPLY WITH SUBPOENA AND SUBPOENA DUCES TECUM SHALL AUTHORIZE THE FILING OF A CASE FOR INDIRECT CONTEMPT UNDER THE RULES OF COURT WITH THE REGIONAL TRIAL COURT AND OBSTRUCTION OF JUSTICE.

Section 17. ESTABLISHMENT OF NATIONAL ANTI-SCAM HUB (NASH). –

THERE SHALL BE ESTABLISHED A COLLABORATIVE NASH MANAGED AND COORDINATED BY THE NCPIA THAT WILL SEEK TO DISRUPT SCAM OPERATIONS, ASSIST IN RECOVERY AND MITIGATION OF VICTIMS' LOSSES, AND FAST-TRACK THE INVESTIGATIONS OF SCAM-RELATED CRIMES, IN COLLABORATION WITH LAW ENFORCEMENT AUTHORITIES, BANKS, TELECOMMUNICATIONS COMPANIES, ONLINE PLATFORMS, FINANCIAL TECHNOLOGY COMPANIES, OPERATORS OF PAYMENT SYSTEMS, AND OTHER STAKEHOLDERS. THESE STAKEHOLDERS, FOLLOWING BEST STANDARDS AND PRACTICES, SHALL CO-LOCATE IN THE NASH FACILITY TO RENDER THE ACTIONS AND THEIR RESULTS IMMEDIATE AND MORE EFFECTIVE.

THE NACC MAY ISSUE THE NECESSARY CIRCULARS OR ORDERS TO OPERATIONALIZE THE NASH TAKING INTO ACCOUNT GLOBAL BEST PRACTICES WITHIN THE FRAMEWORK OF RA 12010, OR THE ANTI-FINANCIAL ACCOUNT AND SCAMMING ACT.

Section 18. REGULATORY AUTHORITY OVER SOCIAL MEDIA PLATFORMS AND OVER-THE-TOP APPLICATIONS TO PREVENT AND SUPPRESS CYBERCRIME. —

THE NACC IS HEREBY AUTHORIZED AND EMPOWERED TO PROMULGATE RULES, REGULATIONS, AND STANDARDS GOVERNING THE OPERATIONS OF SOCIAL MEDIA PLATFORMS, OVER-THE-TOP (OTT) APPLICATIONS, AND OTHER DIGITAL INTERMEDIARIES OPERATING IN THE PHILIPPINES, FOR THE PURPOSE OF PREVENTING, DETECTING, DISRUPTING, AND SUPPRESSING CYBERCRIME, INCLUDING ONLINE SCAMS, FRAUD, IDENTITY THEFT, AND OTHER CYBER-ENABLED OFFENSES.

IN THE EXERCISE OF THIS AUTHORITY, THE NACC SHALL BE GUIDED BY THE FOLLOWING STANDARDS:

1. PUBLIC PROTECTION AND DIGITAL TRUST. — RULES SHALL BE DIRECTED TOWARD THE PROTECTION OF THE PUBLIC, THE PRESERVATION OF TRUST IN DIGITAL SYSTEMS, AND THE INTEGRITY OF THE DIGITAL ECONOMY.
2. RISK-BASED AND PROPORTIONATE REGULATION. — REGULATORY MEASURES SHALL BE PROPORTIONATE, TECHNOLOGY-NEUTRAL, AND RISK-BASED, TAKING INTO ACCOUNT THE SIZE, REACH, AND FUNCTIONAL ROLE OF THE PLATFORM OR APPLICATION IN ENABLING OR MITIGATING CYBERCRIME.
3. PREVENTION, DISRUPTION, AND RAPID RESPONSE. — REGULATIONS SHALL PRIORITIZE EARLY DETECTION, SWIFT DISRUPTION, AND TIMELY RESPONSE TO CYBERCRIME THREATS, INCLUDING OBLIGATIONS RELATING TO NOTICE-AND-ACTION MECHANISMS, CONTENT MODERATION FOR ILLEGAL ACTIVITIES, AND COOPERATION IN EMERGENCY TAKEDOWN OR BLOCKING PROCEDURES.
4. ACCOUNTABILITY AND COOPERATION. — SOCIAL MEDIA PLATFORMS AND OTT APPLICATIONS SHALL BE REQUIRED TO MAINTAIN CLEAR POINTS OF CONTACT, COOPERATE WITH LAWFUL REQUESTS OF COMPETENT AUTHORITIES, PRESERVE RELEVANT DATA SUBJECT TO DUE PROCESS, AND IMPLEMENT REASONABLE SAFEGUARDS AGAINST THE MISUSE OF THEIR SERVICES FOR CRIMINAL ACTIVITY.
5. DUE PROCESS AND FUNDAMENTAL RIGHTS. — ALL REGULATORY MEASURES SHALL RESPECT CONSTITUTIONAL RIGHTS, INCLUDING FREEDOM OF EXPRESSION, PRIVACY, AND DUE PROCESS, AND SHALL ENSURE TRANSPARENCY, ACCOUNTABILITY, AND AVENUES FOR REDRESS.

6. INTER-AGENCY COORDINATION AND INTERNATIONAL ALIGNMENT. — RULES SHALL BE FORMULATED IN COORDINATION WITH RELEVANT GOVERNMENT AGENCIES AND, WHERE APPROPRIATE, ALIGNED WITH INTERNATIONAL STANDARDS, TREATIES, AND BEST PRACTICES TO WHICH THE PHILIPPINES IS A PARTY.

7. CONSULTATIVE AND ADAPTIVE GOVERNANCE. — THE NACC SHALL ADOPT A CONSULTATIVE APPROACH IN RULE-MAKING, ENGAGING STAKEHOLDERS FROM GOVERNMENT, INDUSTRY, CIVIL SOCIETY, AND THE TECHNICAL COMMUNITY, AND SHALL PERIODICALLY REVIEW AND UPDATE REGULATIONS IN LIGHT OF EVOLVING TECHNOLOGIES AND CYBERCRIME TRENDS.

RULES PROMULGATED UNDER THIS SECTION SHALL BE WITHOUT PREJUDICE TO EXISTING REGULATORY POWERS OF OTHER GOVERNMENT AGENCIES AND SHALL BE HARMONIZED WITH APPLICABLE LAWS, INCLUDING THOSE ON DATA PRIVACY, TELECOMMUNICATIONS, COMPETITION, AND ELECTRONIC COMMERCE.

SECTION 19. INITIATING THE COMPLAINT. – NOTWITHSTANDING ANY EXISTING LAWS AND PROCEDURES, IN VIEW OF THE NATURE OF CYBERCRIME, COMPLAINTS ON ANY OFFENSE PUNISHABLE UNDER THIS ACT MAY BE FILED BY THE FOLLOWING:

- (1) PRIVATE COMPLAINANT; OR
- (2) ANY LAW ENFORCEMENT OFFICER IN CASES WHERE THE PRIVATE COMPLAINANT IS LOCATED OUTSIDE OF THE PHILIPPINES AND IS UNABLE TO APPEAR BEFORE THE PROSECUTOR’S OFFICE OR THE COURT.

PRIVATE COMPLAINANT INCLUDES ALL THE SERVICE PROVIDERS AS DEFINED IN SECTION 3(r), AS AMENDED, INCLUDING THOSE PROVIDING BUSINESS PROCESS OUTSOURCING AND SIMILAR SERVICES. FILING

MADE UNDER THIS SUBSECTION (1) SHALL NOT REQUIRE ANY PREREQUISITE ACTION INCLUDING THAT THE SAME BE PRECEDED BY A REPORT OR COMPLAINT FILED WITH A LAW ENFORCEMENT AGENCY.

Section 20. Real-Time Collection of Traffic Data. — Law enforcement authorities, with due cause, UPON SECURING A COURT WARRANT, MAY shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

Traffic data refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

~~All other data to be collected or seized or disclosed require a court warrant.~~

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed: (2) that there are reasonable grounds

to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

Section 21. Preservation of Computer Data. — The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one-time extension for another six (6) months: Provided, That once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

The service provider ordered to preserve computer data shall keep confidential the order and its compliance.

Section 22. Disclosure of Computer Data. — Law enforcement authorities, THROUGH A SUBPOENA OR upon securing a court warrant, shall issue an order requiring any person or service provider, OR INTERNET INTERMEDIARIES, INCLUDING BUT NOT LIMITED TO SOCIAL MEDIA PLATFORMS, MESSAGING CHANNELS, OR WEBSITES, to disclose or submit subscriber's information, traffic data, CONTENT DATA, or relevant data in his/its possession or control within seventy- two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation BEFORE THE LAW ENFORCEMENT AGENCY OR AUTHORITY and the disclosure is necessary and relevant for the purpose of investigation.

Section 23. Search, Seizure and Examination of Computer Data. — Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties:

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:

- (a) To secure a computer system or a computer data storage medium;
- (b) To make and retain a copy of those computer data secured;
- (c) To maintain the integrity of the relevant stored computer data;
- (d) To conduct forensic analysis or examination of the computer data storage medium; and
- (e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination.

Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

SECTION 24. APPLICATION OF CYBERCRIME WARRANTS. – The cybercrime warrants required under this Act shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed: (2) that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

SECTION 25. CUSTODY, PRESERVATION, AND STORAGE OF COMPUTER DATA. — ALL COMPUTER DATA, INCLUDING CONTENT AND TRAFFIC DATA, LAWFULLY OBTAINED, EXAMINED, OR SEIZED PURSUANT TO A VALID WARRANT SHALL, WITHIN FORTY-EIGHT (48) HOURS AFTER THE EXPIRATION OF THE PERIOD FIXED THEREIN, BE SECURELY PRESERVED AND DEPOSITED WITH THE COURT OR, WHERE TECHNICALLY NECESSARY, STORED IN AN ACCREDITED DIGITAL EVIDENCE REPOSITORY UNDER THE CONTROL OF THE COURT OR A DESIGNATED JUDICIAL CUSTODIAN, IN A MANNER THAT ENSURES THE INTEGRITY, AUTHENTICITY, CONFIDENTIALITY, AND ADMISSIBILITY OF SUCH DATA.

THE DEPOSIT SHALL BE ACCOMPANIED BY A SWORN AFFIDAVIT OF THE LAW ENFORCEMENT AUTHORITY EXECUTING THE WARRANT, STATING THE DATES AND TIMES COVERED BY THE EXAMINATION, THE IDENTITY

OF THE OFFICERS WHO ACCESSED OR HANDLED THE DATA, THE METHODS OF EXTRACTION AND PRESERVATION EMPLOYED, THE HASH VALUES OR OTHER INTEGRITY VERIFICATION MEASURES USED, AND SUCH OTHER RELEVANT INFORMATION AS MAY BE REQUIRED TO ESTABLISH AN UNBROKEN CHAIN OF CUSTODY.

WHERE THE VOLUME, FORMAT, OR TECHNICAL NATURE OF THE COMPUTER DATA MAKES PHYSICAL SUBMISSION IMPRACTICABLE, THE COURT MAY AUTHORIZE SECURE ELECTRONIC SUBMISSION, ENCRYPTED STORAGE, OR RETENTION IN A CERTIFIED DIGITAL FORENSIC FACILITY, SUBJECT TO STRICT ACCESS CONTROLS, AUDIT LOGS, AND INTEGRITY-PRESERVATION MECHANISMS IN ACCORDANCE WITH INTERNATIONALLY ACCEPTED DIGITAL EVIDENCE HANDLING STANDARDS.

LAW ENFORCEMENT AUTHORITIES SHALL BE AUTHORIZED TO RETAIN AND USE FORENSIC COPIES OF THE COMPUTER DATA STRICTLY FOR PURPOSES OF INVESTIGATION, PROSECUTION, COURT PROCEEDINGS, AND OFFICIAL RECORD-KEEPING, PROVIDED THAT SUCH COPIES REMAIN CONFIDENTIAL, ACCESS-RESTRICTED, AND PROTECTED AGAINST ALTERATION, DELETION, OR UNAUTHORIZED DISCLOSURE. ANY ACCESS, DUPLICATION, ANALYSIS, OR TRANSFER OF THE COMPUTER DATA SHALL BE PROPERLY DOCUMENTED AND SUBJECT TO JUDICIAL OVERSIGHT TO ENSURE THE CONTINUED INTEGRITY AND EVIDENTIARY VALUE OF THE DIGITAL EVIDENCE.

Section 26. Exclusionary Rule. — Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

~~***Section 23. Restricting or Blocking Access to Computer Data.***~~ — When a computer data is prima facie found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data..

SECTION 27. CONFIDENTIALITY IN HANDLING THIRD-PARTY DATA OR INFORMATION DURING CYBERCRIME INVESTIGATIONS AND PROCEEDINGS. – AN ENTITY ENGAGED IN THE COLLECTION, PROCESSING, HANDLING, STORAGE, OR TRANSMISSION OF PERSONAL, SENSITIVE, AND PROPRIETARY INFORMATION BELONGING TO A THIRD PARTY, INCLUDING BUT NOT LIMITED TO BUSINESS PROCESS OUTSOURCING (BPO) COMPANIES AND INFORMATION TECHNOLOGY (IT) SERVICE PROVIDERS, SHALL OBSERVE STRICT CONFIDENTIALITY OVER SUCH INFORMATION, EVEN IN THE EVENT THAT SUCH DATA BECOMES RELEVANT TO A CYBERCRIME INVESTIGATION OR LEGAL PROCEEDING.

Section 28. Non-compliance. — Failure to comply with the provisions of Chapter IV hereof, specifically the orders from law enforcement authorities, shall be punished with imprisonment of prision correccional in its maximum period or a fine of THREE HUNDRED THOUSAND PESOS (PHP300,00.00) or both, for each and every non-compliance with an order issued by law enforcement authorities WITHOUT PREJUDICE TO THE PROVISIONS OF PRESIDENTIAL DECREE NO. 1829.

CHAPTER V JURISDICTION

Section 29. Jurisdiction. — The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act, including any violation committed by a Filipino national, regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

CHAPTER VI

INTERNATIONAL COOPERATION

Section 30. General Principles Relating to International Cooperation. — All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal, offense shall be given full force and effect.

Section 31. Department of Justice (DOJ). — There is hereby created an Office of Cybercrime within the DOJ designated as the central authority in all matters related to international mutual LEGAL assistance and extradition.

SECTION 32. COOPERATION WITH FOREIGN LAW ENFORCEMENT AGENCIES IN CYBERCRIME INVESTIGATION. — RECOGNIZING THE TRANSNATIONAL NATURE OF CYBERCRIME, THE NCPIA, IN COORDINATION WITH PNP AND NBI, SHALL ENDEAVOR TO ESTABLISH COOPERATION ARRANGEMENTS WITH FOREIGN LAW ENFORCEMENT AGENCIES FOR FASTER EXCHANGE OF INFORMATION, INTELLIGENCE, BEST PRACTICES, AND JOINT INVESTIGATIONS ON VIOLATIONS OF THIS ACT.

CHAPTER VII

NCPIA'S ORGANIZATIONAL FRAMEWORK AND FINAL PROVISIONS

SECTION 33. REGIONAL OFFICES OF NCPIA. – THE NCPIA MAY ESTABLISH, OPERATE, AND MAINTAIN A REGIONAL OFFICE IN THE DIFFERENT ADMINISTRATIVE REGIONS OF THE COUNTRY AS THE NEED ARISES, SUBJECT TO APPROVAL OF NACC AND CONCURRENCE OF DEPARTMENT OF BUDGET AND MANAGEMENT (DBM). EACH REGIONAL OFFICE SHALL BE HEADED BY A REGIONAL DIRECTOR, WHO MAY BE ASSISTED BY ONE (1) ASSISTANT REGIONAL DIRECTOR. THE REGIONAL DIRECTOR AND ASSISTANT REGIONAL DIRECTOR SHALL BE APPOINTED BY THE PRESIDENT. THE REGIONAL OFFICES SHALL ENSURE THE

PERFORMANCE OF THE FUNCTIONS AND RESPONSIBILITIES OF THE NCPIA IN THEIR RESPECTIVE ADMINISTRATIVE REGIONS.

SECTION 34. COMPENSATION AND OTHER EMOLUMENTS FOR NCPIA OFFICIALS AND PERSONNEL. – TO ENSURE THAT THE NCPIA WILL ATTRACT THE NECESSARY EXPERTISE AND TALENTS GIVEN ITS HIGHLY TECHNICAL MANDATE, THE COMPENSATION AND OTHER EMOLUMENTS OF ITS OFFICIALS AND PERSONNEL SHALL BE EXEMPTED FROM THE COVERAGE OF RA 6758, OTHERWISE KNOWN AS THE “SALARY STANDARDIZATION ACT,” AS AMENDED. FOR THIS PURPOSE, THEIR SALARIES AND EMOLUMENTS SHALL BE SET BASED ON AN OBJECTIVE CLASSIFICATION SYSTEM, TAKING INTO CONSIDERATION THE HIGHLY SPECIALIZED NATURE OF, IMPORTANCE, AND RESPONSIBILITIES ATTACHED TO THE RESPECTIVE POSITIONS, AND SHALL BE SUBMITTED TO THE PRESIDENT OF THE PHILIPPINES FOR HIS APPROVAL.

SECTION 35. ABOLITION OF CICC AND TRANSFER OF PERSONNEL. – THE CICC IS HEREBY ABOLISHED, ITS APPLICABLE FUNDS AND APPROPRIATIONS, RECORDS, EQUIPMENT, PROPERTY, AND PERSONNEL ARE TRANSFERRED TO THE NCPIA.

SECTION 36. 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 ABOLITION OF CICC UNDER THE PROVISIONS OF THIS ACT SHALL RECEIVE SEPARATION BENEFITS TO WHICH THEY MAY BE ENTITLED.

SECTION 37. STRUCTURE AND STAFFING PATTERN. – SUBJECT TO THE APPROVAL OF THE DBM AND THE OFFICE OF THE PRESIDENT, THE NCPIA SHALL DETERMINE ITS ORGANIZATIONAL STRUCTURE AND CREATE NEW DIVISIONS OR UNITS AS IT MAY DEEM NECESSARY, AND SHALL APPOINT OFFICERS AND EMPLOYEES OF THE NCPIA IN ACCORDANCE WITH THE CIVIL SERVICE LAW, RULES, AND REGULATIONS. THE NAME OF THE POSITIONS AND DESCRIPTION OF QUALIFICATION STANDARDS RELATING TO THE NEW TABLE OF

ORGANIZATION SHALL TAKE INTO ACCOUNT THE TECHNICAL NATURE THEREOF INCLUDING THE REASONABLE COMPENSATION LEVEL AS PREVAILING IN THE SECTOR, AMONG OTHERS.

SECTION 38. TRANSITION PERIOD. – THE TRANSFER OF ASSETS, FUNDS, EQUIPMENT, PROPERTIES, TRANSACTIONS, AND PERSONNEL OF CICC, AND THE FORMULATION OF THE INTERNAL ORGANIC STRUCTURE, STAFFING PATTERN, OPERATING SYSTEM, AND REVISED BUDGET OF NCPIA, SHALL BE COMPLETED WITHIN TWO (2) YEARS FROM THE EFFECTIVITY OF THIS ACT, DURING WHICH TIME, THE EXISTING PERSONNEL SHALL CONTINUE TO ASSUME THEIR POSTS IN HOLDOVER CAPACITIES UNTIL NEW APPOINTMENTS ARE ISSUED: *PROVIDED*, THAT AFTER THE ABOLITION OF CICC AS SPECIFIED IN SECTION 34 OF THIS ACT, THE NCPIA, IN COORDINATION WITH THE DBM, SHALL DETERMINE AND CREATE NEW POSITIONS AS PRESCRIBED IN SECTION 36 OF THIS ACT: *PROVIDED*, FURTHER, THAT REFERENCE TO NCPIA, PARTICULARLY IN THE FORMULATION OF IRR, SHALL REFER TO THE HOLD-OVER OFFICIALS FROM CICC.

Section 39. Appropriations. — THE AMOUNT OF AT LEAST NINE HUNDRED EIGHTY MILLION PESOS (PHP 980,000,000.00) SHALL BE APPROPRIATED ANNUALLY FOR THE IMPLEMENTATION OF THIS ACT.

THEREAFTER, SUCH AMOUNTS NECESSARY FOR THE IMPLEMENTATION OF THIS ACT SHALL BE INCLUDED IN THE ANNUAL GENERAL APPROPRIATIONS ACT (GAA).

SECTION 40. ANNUAL REPORT. – THE NCPIA, THROUGH NACC, SHALL SUBMIT TO THE OFFICE OF THE PRESIDENT, THE SENATE AND THE HOUSE OF REPRESENTATIVES, WITHIN THE FIRST QUARTER OF THE SUCCEEDING YEAR, AN ANNUAL REPORT RELATING TO THE PROGRESS OF THE IMPLEMENTATION OF THIS ACT.

SECTION 41. IMPLEMENTING RULES AND REGULATIONS. — THE DICT, NCPIA, NTC, PNP, NBI, BSP, DTI, DOJ-OOC AND AMLC SHALL FORMULATE

THE NECESSARY RULES AND REGULATIONS WITHIN NINETY (90) DAYS FROM APPROVAL OF THIS ACT, FOR ITS EFFECTIVE IMPLEMENTATION.

SECTION 42. MANDATORY REVIEW BY THE REORGANIZATION AND REVIEW COMMISSION. – FIVE (5) YEARS AFTER THE EFFECTIVITY OF THIS ACT, OR AS THE NEED ARISES, THE PRESIDENT SHALL CONSTITUTE A REORGANIZATION AND REVIEW COMMISSION WHICH SHALL CONDUCT A SYSTEMATIC EVALUATION OF THE ACCOMPLISHMENTS AND IMPACT OF THIS ACT, AS WELL AS THE PERFORMANCE AND ORGANIZATIONAL STRUCTURE OF NCPIA, FOR PURPOSES OF DETERMINING REMEDIAL LEGISLATION. IN THE CONDUCT OF THIS SYSTEMATIC EVALUATION, THE COMMISSION SHALL SPEARHEAD AND FACILITATE THE HOLDING OF IN-DEPTH CONSULTATIONS WITH GOVERNMENT AGENCIES, LAW ENFORCEMENT UNITS, INDUSTRY STAKEHOLDERS SUCH AS SERVICE PROVIDERS, ICT AND BPO SECTORS, CIVIL SOCIETY ORGANIZATIONS, AND OTHER RELEVANT PARTNERS TO ENSURE AN EVIDENCE-BASED AND DATA-BACKED ANALYSIS RESPONSIVE TO EVOLVING CYBERCRIME THREATS. THE EVALUATION REPORT SHALL BE RELEASED AND MADE AVAILABLE TO STAKEHOLDERS AND THE PUBLIC.

THE COMMISSION SHALL BE COMPOSED OF THE OFFICE OF THE EXECUTIVE SECRETARY, SECRETARY OF THE DICT, THE DIRECTOR GENERAL OF NCPIA, DIRECTOR OF THE NBI, CHIEF OF THE PNP, AND THE SECRETARY OF DBM.

SECTION 43. SEPARABILITY CLAUSE. — IF ANY PROVISION OF THIS ACT IS HELD INVALID, THE OTHER PROVISIONS NOT AFFECTED SHALL REMAIN IN FULL FORCE AND EFFECT.

SECTION 44. REPEALING CLAUSE. — ALL LAWS, EXECUTIVE ORDERS, ISSUANCES, RULES AND REGULATIONS, OR PARTS THEREOF INCONSISTENT WITH THE PROVISIONS OF THIS ACT ARE REPEALED OR MODIFIED ACCORDINGLY.

Section 45. Effectivity. — This Act shall take effect fifteen (15) days after THE COMPLETION OF its publication in the Official Gazette or in a newspaper of general circulation.

Approved,


HON. BRIAN POE, PhD, MNSA
Representative
FPJ Panday Bayanihan Party-List