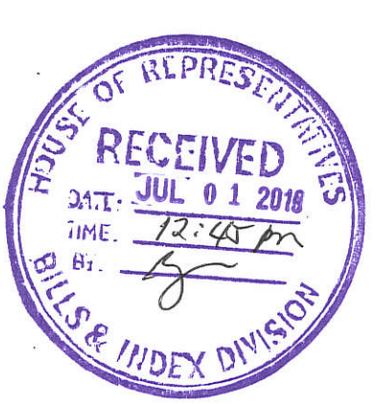
EIGHTEENTH CONGRESS)
OF THE REPUBLIC OF THE PHILIPPINES)
First Regular Session)



HOUSE OF REPRESENTATIVES

House Bill No. 359

Introduced by Representative Victor A. Yap

EXPLANATORY NOTE

Despite the passage of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012, the incidence of cyber-enabled offenses is still on the rise. The number of cybercrime cases in the country has increased by 80 percent—from 2,284 cases in 2017 to 4,103 cases in 2018—according to the Philippine National Police Anti-Cybercrime Group (PNP-ACG).

While the PNP-ACG downplayed the increase, saying it only shows people's awareness of the different cybercrimes and reporting these incidents to the authorities, law enforcement authorities have admitted that thwarting cybercrime remains a challenge for them as they have to constantly adjust their strategies due to the rapidly evolving technology.

This bill aims to empower the law enforcement agencies by mandating the PNP, the National Bureau of Investigation, and the Department of Justice to create their own cybercrime divisions to ensure the strict implementation of the Cybercrime Prevention Law. It also allows law enforcement authorities, upon securing a court warrant, to conduct interception and collection of traffic and content data, which are held or maintained by a cloud computing service provider situated outside the Philippines.

In addition to the imposable imprisonment and fine, this proposed measure seeks to suspend and limit the right to access the internet of any person found guilty of cybercrime.

In the interest of our people's security, support for the passage of this bill is earnestly sought.

VICTOR A. YAP
Representative, 2nd District of Tarlac

EIGHTEENTH CONGRESS)
OF THE REPUBLIC OF THE PHILIPPINES)
First Regular Session **)**

HOUSE OF REPRESENTATIVES

House Bill No. 359

Introduced by Representative Victor A. Yap

AN ACT
AMENDING REPUBLIC ACT 10175, OTHERWISE KNOWN AS THE "CYBERCRIME PREVENTION ACT OF 2012," AND FOR OTHER PURPOSES

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

SECTION 1. Section 3 of the Cybercrime Prevention Act of 2012 is hereby amended by inserting paragraphs (q) and (r) to read as follows:

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

x xx

(Q) "COMMITTED BY, THROUGH AND WITH THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES" REFERS TO THE COMMISSION OF A CRIME DEFINED AND PENALIZED BY THE REVISED PENAL CODE, AS AMENDED, AND SPECIAL LAWS, IN WHICH ANY OF ITS ELEMENTS ARE COMMITTED BY, THROUGH AND WITH THE USE OF ANY ELECTRONIC DEVICE, WHICH CAN ACCESS, CREATE, STORE, PROCESS, RECEIVE, TRANSMIT, PRESENT, AND DISSEMINATE INFORMATION;" AND

(R) "CLOUD" OR "CLOUD COMPUTING" REFERS TO STORING, ACCESSING, AND/OR PROCESSING DATA AND/OR PROGRAMS OVER THE INTERNET, PROVIDED BY A PERSON WHO MAINTAINS THE SOFTWARE AND/OR DATA STORAGE FACILITIES, WHICH COULD BE AT A NEARBY DATA CENTER,

SPREAD OUT OVER MULTIPLE DATA CENTERS, OR STORED IN FOREIGN COUNTRIES."

SECTION 2. A new section shall be inserted after Section 8 to read as follows:

"SEC. 8-A. TEMPORARY DISQUALIFICATION TO ACCESS THE INTERNET. – IN ADDITION TO THE IMPOSABLE IMPRISONMENT AND/OR FINE MENTIONED IN THE IMMEDIATELY PRECEDING SECTION, ANY PERSON FOUND GUILTY OF ANY OF THE PUNISHABLE ACTS ENUMERATED IN THIS ACT SHALL BE DEPRIVED THE RIGHT TO ACCESS THE INTERNET.

THE RIGHT OF THE ACCUSED OF ANY OF THE PUNISHABLE ACTS HEREIN TO ACCESS THE INTERNET MAY BE SUSPENDED OR LIMITED BY THE CYBERCRIME COURT PENDING FINAL JUDGMENT UPON SHOWING, WITH DUE NOTICE AND HEARING, THAT THERE IS A STRONG LIKELIHOOD THAT THE ACCUSED WILL BE ABLE TO FACILITATE THE COMMISSION OF THE OFFENSE SO CHARGED UNLESS SUCH ORDER WAS ISSUED.

THE SUSPENSION OF THE RIGHT TO ACCESS THE INTERNET SHALL LAST DURING THE TERM OF THE SENTENCE OF THE CONVICT."

SECTION 3. Section 10 of the same Act is hereby amended to read as follows:

"SEC. 10. [*Law*] *Enforcement Authorities.* – [The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations] THERE IS HEREBY CREATED AN ANTI-CYBERCRIME GROUP IN THE PHILIPPINE NATIONAL POLICE (PNP), A CYBERCRIME DIVISION IN THE NATIONAL BUREAU OF INVESTIGATION (NBI), AND AN OFFICE OF CYBERCRIME WITHIN THE DEPARTMENT OF JUSTICE (DOJ) TO IMPLEMENT THE PROVISIONS of this Act."

SECTION 4. Section 11 of the same Act is hereby amended to read as follows:

"SEC. 11. *DUTIES AND FUNCTIONS OF THE PNP-ANTI-CYBERCRIME GROUP AND THE NBI CYBERCRIME DIVISION.* [Duties of Law Enforcement Authorities.] — [To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.] THE PNP ANTI-CYBERCRIME GROUP AND THE NBI CYBERCRIME DIVISION SHALL HAVE THE FOLLOWING DUTIES AND FUNCTIONS:

(A) TO INVESTIGATE THE PROHIBITED ACTS UNDER CHAPTER II AND TO SUPPORT INVESTIGATIONS WHERE COMPUTER SYSTEMS ARE INVOLVED INCLUDING THE SEARCH, SEIZURE, EVIDENCE PRESERVATION, FORENSIC RECOVERY OF DATA FROM CRIME SCENES AND SYSTEMS USED IN CRIMES;

(B) TO CONDUCT DATA RECOVERY AND FORENSIC ANALYSIS ON COMPUTER SYSTEMS AND OTHER ELECTRONIC EVIDENCE SEIZED AS PROVIDED UNDER CHAPTER IV OF THIS ACT;

(C) TO FORMULATE GUIDELINES IN INVESTIGATION, FORENSIC EVIDENCE RECOVERY, AND FORENSIC DATA ANALYSIS CONSISTENT WITH INDUSTRY STANDARD AND INTERNATIONAL BEST PRACTICES;

(D) TO DEVELOP CAPACITY WITHIN THEIR ORGANIZATIONS INCLUDING EXTENDING TECHNICAL SUPPORT AND TO PERFORM SUCH

DUTIES NECESSARY FOR THE ENFORCEMENT OF THIS ACT; AND

(E) TO MAINTAIN DATABASE OF THE COMPLAINTS RECEIVED AND SUBMIT TIMELY AND REGULAR REPORTS PERTAINING THERETO, INCLUDING PRE-OPERATION, POST-OPERATION AND INVESTIGATION RESULTS, AND SUCH OTHER DOCUMENTS AS MAY BE REQUIRED TO THE DOJ – OFFICE OF CYBERCRIME FOR REVIEW AND MONITORING, TO ENSURE THAT THE TECHNICAL NATURE OF CYBERCRIME AND ITS PREVENTION IS GIVEN FOCUS AND CONSIDERING THE PROCEDURES INVOLVED FOR INTERNATIONAL COOPERATION.

THE PNP ANTI-CYBERCRIME GROUP AND THE NBI CYBERCRIME DIVISION SHALL RESPECTIVELY BE HEADED BY AT LEAST A POLICE DIRECTOR (2-STAR RANK) AND A DIRECTOR II."

SECTION 5. New sections shall be inserted after Section 11 to read as follows:

"SEC. 11-A. *CYBERCRIME INVESTIGATION.* – ALL CYBERCRIME INVESTIGATIONS SHALL BE COORDINATED WITH THE DOJ – OFFICE OF CYBERCRIME. DURING CYBERCRIME INVESTIGATIONS, THE DOJ – OFFICE OF CYBERCRIME SHALL ACT AS A COMPETENT AUTHORITY FOR ALL REQUESTS FOR ASSISTANCE FOR INVESTIGATION OR PROCEEDINGS CONCERNING CYBERCRIMES, INCLUDING THE PROVISION OF LEGAL AND/OR TECHNICAL ADVICE.

SEC. 11-B. *INVESTIGATING PROSECUTORS IN CYBERCRIME INVESTIGATIONS.* – THERE SHALL BE SPECIALLY TRAINED PROSECUTORS FROM THE DOJ NATIONAL PROSECUTION SERVICE ASSIGNED TO THE DOJ

– OFFICE OF CYBERCRIME TO DIRECTLY CONTROL AND SUPERVISE CYBERCRIME INVESTIGATIONS.

LAW ENFORCERS SHALL TAKE GUIDANCE FROM, AND COOPERATE CLOSELY, WITH THE INVESTIGATING PROSECUTOR IN THE PROCESS OF CONDUCTING CYBERCRIME INVESTIGATIONS, ESPECIALLY IN MATTERS CONCERNING COMPLIANCE WITH LAWS AND RULES OF PROCEDURE, EVIDENCE-GATHERING, AND CASE-BUILD UP AND OPERATIONS.

SEC. 11-C. *POWERS OF THE INVESTIGATING PROSECUTOR DURING CYBERCRIME INVESTIGATIONS.* – THE INVESTIGATING PROSECUTOR SHALL EXERCISE THE FOLLOWING POWERS DURING CYBERCRIME INVESTIGATIONS:

(A) INITIATE, MANAGE AND SUPERVISE ALL INCIDENTS OF THE CYBERCRIME INVESTIGATION, IN COORDINATION WITH CONCERNED ENFORCEMENT AUTHORITIES;

(B) PERFORM ALL ACTS NECESSARY TO ENSURE THE INTEGRITY OF THE CYBERCRIME INVESTIGATION PROCESS AND ITS COMPLIANCE WITH RELEVANT LAWS AND RULES;

(C) ENSURE THE INTEGRITY OF THE CHAIN OF CUSTODY OVER EVIDENCE AT ALL STAGES OF THE CYBERCRIME INVESTIGATION;

(D) CAUSE THE APPLICATION FOR COURT WARRANTS FOR SEARCH, SEIZURE, EXAMINATION, INTERCEPTION AND COLLECTION, AND DISCLOSURE OF COMPUTER DATA, AND SUCH OTHER PROCESSES AS MAY

BE NECESSARY IN THE COURSE OF THE CYBERCRIME INVESTIGATION; AND

(E) DIRECT LAW ENFORCERS TO SUBMIT INVENTORIES, REPORTS, FINDINGS AND OTHER DOCUMENTS, AS MAY BE REQUIRED, IN CONNECTION WITH THE CYBERCRIME INVESTIGATION.

THE FOREGOING NOTWITHSTANDING, NO INVESTIGATING PROSECUTOR SHALL FORM PART OF THE DOJ PROSECUTION TASK FORCE ON CYBERCRIME WHOSE PRIMARY DUTY CONSISTS OF DETERMINING PROBABLE CAUSE, AND THE PROSECUTION OF THE OFFENDERS, IN CYBERCRIME AND CYBER-RELATED CASES."

Section 6. Section 12 of the same Act is hereby amended to read as follows:

"SEC 12. INTERCEPTION AND COLLECTION OF COMPUTER DATA. [Real-Time Collection of Traffic Data. – Law enforcement authorities, with due cause, 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 will 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.]

LAW ENFORCEMENT AUTHORITIES SHALL, UPON SECURING A COURT WARRANT, BE AUTHORIZED TO CONDUCT INTERCEPTION AND/OR COLLECTION OF TRAFFIC AND CONTENT DATA.

THIS ALSO APPLIES TO THE CONDUCT OF INTERCEPTION AND/OR COLLECTION BY LAW ENFORCEMENT AUTHORITIES OF TRAFFIC AND CONTENT DATA THAT IS HELD OR MAINTAINED BY A CLOUD COMPUTING SERVICE PROVIDER SITUATED OUTSIDE THE PHILIPPINES EITHER:

(A) ON BEHALF OF, AND RECEIVED BY MEANS OF ELECTRONIC TRANSMISSION FROM OR CREATED BY MEANS OF COMPUTER PROCESSING OF COMMUNICATIONS RECEIVED BY MEANS OF ELECTRONIC TRANSMISSION FROM, A SUBSCRIBER OR CUSTOMER OF SUCH CLOUD COMPUTING SERVICE; AND

(B) SOLELY FOR THE PURPOSE OF PROVIDING STORAGE OR COMPUTER PROCESSING SERVICES TO SUCH SUBSCRIBER OR CUSTOMER, IF THE PROVIDER IS NOT AUTHORIZED TO ACCESS THE CONTENTS OF ANY SUCH COMMUNICATIONS FOR PURPOSES OF PROVIDING ANY SERVICES OTHER THAN STORAGE OR COMPUTER PROCESSING.

THE SERVICE OF THE COURT WARRANT MENTIONED IN THE IMMEDIATELY PRECEDING PARAGRAPH SHALL BE COURSED THROUGH THE DOJ – OFFICE OF CYBERCRIME, IN LINE WITH ITS DUTY AS THE CENTRAL AUTHORITY.

SERVICE PROVIDERS ARE REQUIRED TO COOPERATE AND ASSIST LAW ENFORCEMENT AUTHORITIES IN THE COLLECTION OR RECORDING OF THE ABOVE-STATED INFORMATION.

THE FOREGOING NOTWITHSTANDING, ANY ENFORCEMENT AUTHORITY OR ANY PERSON, WHO IS A PARTY TO A COMMUNICATION SUBJECT OF A SPECIFIED COMPUTER DATA, MAY GIVE HIS CONSENT TO AND/OR AUTHORIZE SUCH INTERCEPTION AND COLLECTION, AND MAY REQUIRE THE PERSON OR SERVICE PROVIDER TO COLLECT OR RECORD BY TECHNICAL OR ELECTRONIC MEANS THE NECESSARY DATA AND/OR TO COOPERATE OR ASSIST IN THE COLLECTION OR RECORDING OF COMPUTER DATA.

IN ALL INSTANCES, IT SHALL BE ENSURED THAT THE DATA TO BE COLLECTED OR RECORDED SHALL BE LIMITED EITHER TO THE DATA DESCRIBED IN THE COURT WARRANT OR TO THE SPECIFIED COMMUNICATION TO WHICH THEY ARE A PARTY TO."

SECTION 7. Section 15 of the same Act is hereby amended to read as follows:

"SEC. 15. *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) SEARCH AND SEIZE COMPUTER DATA SUBJECT OF THE COURT WARRANT;

[(a)] (B) [To] S[s]ecure computer system/S or computer data storage [media] MEDIUM;

[(b)] (C) [To] M[m]ake and retain copy of those computer data secured;

[(c)] (D) [To] M[m]aintain the integrity of the relevant stored computer data;

[(d)] (E) [To] C[c]onduct forensic analysis or examination of the computer data storage [medium] MEDIA IN ORDER TO COLLECT AND PRESERVE VOLATILE DATA; and

[(e)] (F) [To] R[r]ender inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, enforcement authorities may order any person who [has] MAY HAVE knowledge of 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] TO ASSIST IN 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.]

THEREAFTER, ENFORCEMENT AUTHORITIES SHALL FORTHWITH MAKE AN INITIAL RETURN TO THE JUDGE WHO ISSUED THE WARRANT, TOGETHER WITH THE INVENTORY OF THE ITEMS SEIZED, INCLUDING THE HASH VALUES OF THE SEIZED COMPUTER DATA AND/OR COMPUTER STORAGE MEDIUM WHERE THE SEIZED COMPUTER DATA ARE STORED. IN CASES WHERE THE TIME ALLOTTED TO CONDUCT FORENSIC EXAMINATION AND ANALYSIS UNDER SUBPARAGRAPH (E) OF THIS SECTION IS NOT SUFFICIENT, ENFORCEMENT AUTHORITIES MAY REQUEST FOR A ONE (1)-TIME EXTENSION OF THIRTY (30) DAYS, SUBJECT TO THE PARTIAL SUBMISSION OF THOSE ALREADY COMPLETED AND PROVIDE A JUSTIFIABLE REASON FOR THE REQUEST OF SUCH EXTENSION. LIKEWISE, IN THEIR INITIAL RETURN, ENFORCEMENT AUTHORITIES SHALL PRAY FOR ALLOWANCE OF PERIOD WITHIN WHICH FULL FORENSIC EXAMINATIONS AND ANALYSES MAY BE CONDUCTED.

WITHIN FORTY-EIGHT (48) HOURS AFTER THE EXPIRATION OF THE PERIOD GRANTED BY THE COURT

UNDER THE IMMEDIATELY PRECEDING PARAGRAPH, ENFORCEMENT AUTHORITIES SHALL FORTHWITH MAKE THE FULL RETURN OF THE WARRANT AND DEPOSIT WITH THE COURT ALL COMPUTER DATA EXAMINED. THE COURT SHALL ASCERTAIN THAT THE HASH VALUES SUBMITTED DURING THE INITIAL RETURN AND THE FULL RETURN ARE THE SAME AND INTACT TO ENSURE THE INTEGRITY OF EVIDENCE WERE PRESERVED."

SECTION 8. Section 23 of the same Act is hereby amended to read as follows:

"SEC. 23. DOJ-Office of Cybercrime. – [There is hereby created an Office of Cybercrime within the DOJ designated as the central authority in all matters related to international mutual assistance and extradition.] THE DOJ – OFFICE OF CYBERCRIME SHALL HAVE THE FOLLOWING DUTIES AND FUNCTIONS:

(A) SERVE AS THE CENTRAL AUTHORITY IN ALL MATTERS RELATED TO INTERNATIONAL MUTUAL ASSISTANCE AND EXTRADITION FOR CYBERCRIME AND CYBER-RELATED CASES, INCLUDING SENDING AND ANSWERING REQUESTS FOR MUTUAL ASSISTANCE, THE EXECUTION OF SUCH REQUESTS OR THEIR TRANSMISSION TO THE AUTHORITIES COMPETENT FOR THEIR EXECUTION;

(B) ACT AS THE PRINCIPAL ADMINISTRATOR AND FOCAL AUTHORITY OF THIS ACT, INCLUDING FORMULATING AND IMPLEMENTING LAW ENFORCEMENT INVESTIGATION AND PROSECUTION STRATEGIES IN CURBING CYBERCRIME AND CYBER-RELATED CASES TO ENSURE THAT THE TECHNICAL NATURE OF CYBERCRIME AND ITS PREVENTION IS GIVEN FOCUS AND CONSIDERING THE PROCEDURES FOR INTERNATIONAL COOPERATION;

(C) ISSUE PRESERVATION ORDERS ADDRESSED TO SERVICE PROVIDERS;

(D) ADMINISTER OATHS, ISSUE SUBPOENA AND SUMMON WITNESSES TO APPEAR IN AN INVESTIGATION OR PROCEEDINGS FOR CYBERCRIME;

(E) REQUIRE THE SUBMISSION OF TIMELY AND REGULAR REPORTS INCLUDING PRE-OPERATION, POST-OPERATION AND INVESTIGATION RESULTS, AND SUCH OTHER DOCUMENTS FROM THE PNP AND NBI FOR MONITORING AND REVIEW;

(F) MONITOR THE COMPLIANCE OF THE SERVICE PROVIDERS WITH THE PROVISIONS OF CHAPTER IV OF THIS ACT;

(G) FACILITATE INTERNATIONAL COOPERATION WITH OTHER AGENCIES ON INTELLIGENCE, TRAINING, AND CAPACITY-BUILDING RELATED TO CYBERCRIME PREVENTION, SUPPRESSION, INVESTIGATION AND PROSECUTION;

(H) ISSUE AND PROMULGATE GUIDELINES, ADVISORIES, AND PROCEDURES IN ALL MATTERS RELATED TO CYBERCRIME INVESTIGATION, FORENSIC EVIDENCE RECOVERY, AND FORENSIC DATA ANALYSIS CONSISTENT WITH INDUSTRY STANDARD PRACTICES;

(I) PRESCRIBE FORMS AND TEMPLATES, INCLUDING, BUT NOT LIMITED TO, THOSE FOR PRESERVATION ORDERS, CHAIN OF CUSTODY, CONSENT TO SEARCH, CONSENT TO ASSUME ACCOUNT/ONLINE IDENTITY, AND REQUEST FOR COMPUTER FORENSIC EXAMINATION; AND

(J) PERFORM SUCH OTHER ACTS NECESSARY FOR THE IMPLEMENTATION OF THIS ACT."

SECTION 9. A new section shall be inserted after Section 23 to read as follows:

"SEC. 23-A. *NATIONAL COMPUTER FORENSICS TRAINING PROGRAM.* – IN RELATION TO SECTION 23 (B) OF THIS ACT, THERE IS HEREBY ESTABLISHED A NATIONAL COMPUTER FORENSICS TRAINING PROGRAM (NCFTP) UNDER THE MANAGEMENT AND SUPERVISION OF THE DOJ – OFFICE OF CYBERCRIME, WHICH SHALL PROVIDE FOR A CONSOLIDATED TRAINING IN COMPUTER FORENSICS AMONG ALL LAW ENFORCEMENT AGENCIES, CONSISTENT WITH INTERNATIONAL BEST PRACTICES.

THE AMOUNT OF FIFTY MILLION PESOS (PHP50,000,000.00) NECESSARY FOR THE IMPLEMENTATION OF THIS PROGRAM SHALL BE APPROPRIATED ANNUALLY IN THE GENERAL APPROPRIATIONS ACT OF DOJ."

SECTION 10. Section 24 of the same Act is hereby amended to read as follows:

"SEC. 24. *CYBERSECURITY INTEGRATION AND PROVISION CENTER. [Cybercrime Investigation and Coordinating Center.]* — [There is hereby created, within thirty (30) days from the effectivity of this Act, an inter-agency body to be known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, for policy coordination among concerned agencies and for the formulation and enforcement of the national cybersecurity plan.] THERE IS HEREBY ESTABLISHED AN INTER-AGENCY BODY TO BE KNOWN AS CYBERSECURITY INTEGRATION AND PROVISION CENTER (CIPC) FOR POLICY COORDINATION AMONG CONCERNED AGENCIES AND FOR THE FORMULATION AND ENFORCEMENT OF THE NATIONAL CYBERSECURITY PLAN."

SECTION 11. Section 25 of the same Act is hereby amended to read as follows:

"SEC. 25. Composition. – [The CICC shall be headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson with the Director of the NBI as Vice Chairperson; the Chief of the PNP; Head of the DOJ Office of Cybercrime; and one (1) representative from the private sector and academe, as members. The CICC shall be manned by a secretariat of selected existing personnel and representatives from the different participating agencies.] THE CIPC SHALL BE CHAIRED BY THE SECRETARY OF THE DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT), CO-CHAIRED BY THE SECRETARY OF THE DEPARTMENT OF JUSTICE AND THE DIRECTOR GENERAL OF THE NATIONAL SECURITY COUNCIL, AND SHALL HAVE THE FOLLOWING AS MEMBERS:

A. SECRETARY, DEPARTMENT OF FOREIGN AFFAIRS;
B. SECRETARY, DEPARTMENT OF ENERGY;
C. SECRETARY, DEPARTMENT OF FINANCE;
D. SECRETARY, DEPARTMENT OF THE INTERIOR AND LOCAL GOVERNMENT (DILG);
E. SECRETARY, DEPARTMENT OF SCIENCE AND TECHNOLOGY;
F. SECRETARY, DEPARTMENT OF NATIONAL DEFENSE;
G. SECRETARY, DEPARTMENT OF TRANSPORTATION;
H. SECRETARY, PRESIDENTIAL COMMUNICATIONS OPERATION OFFICE;
I. CHAIRMAN, NATIONAL PRIVACY COMMISSION;
J. COMMISSIONER, NATIONAL TELECOMMUNICATIONS COMMISSION;
K. EXECUTIVE DIRECTOR, ANTI-TERRORISM COUNCIL;
L. EXECUTIVE DIRECTOR, ANTI-MONEY LAUNDERING COUNCIL;
M. EXECUTIVE DIRECTOR, PHILIPPINE CENTER ON TRANSNATIONAL CRIME;

N. DIRECTOR GENERAL, PHILIPPINE NATIONAL POLICE;

O. DIRECTOR, NATIONAL BUREAU OF INVESTIGATION; AND

P. ONE (1) REPRESENTATIVE EACH FROM THE PRIVATE SECTOR, NON-GOVERNMENTAL ORGANIZATION, AND ACADEME. THESE REPRESENTATIVES SHALL BE NOMINATED BY THE GOVERNMENT AGENCY REPRESENTATIVES OF THE CIPC FOR THE APPOINTMENT BY THE PRESIDENT FOR A TERM OF THREE (3) YEARS.

THE MEMBERS OF THE CIPC MAY DESIGNATE THEIR PERMANENT REPRESENTATIVES WHO SHALL HAVE A RANK NOT LOWER THAN AN ASSISTANT SECRETARY OR ITS EQUIVALENT, TO MEETINGS AND SHALL RECEIVE EMOLUMENTS AS MAY BE DETERMINED BY THE CIPC IN ACCORDANCE WITH EXISTING BUDGET AND ACCOUNTING RULES AND REGULATIONS."

SECTION 12. A new section shall be inserted after Section 25 to read as follows:

"SEC. 25-A. *SECRETARIAT TO THE CIPC.* – THE DICT SHALL ESTABLISH THE NECESSARY SECRETARIAT FOR THE CIPC WHICH SHALL PROVIDE SUPPORT FOR THE FUNCTIONS AND PROJECTS OF THE CIPC.

THE SECRETARIAT SHALL BE HEADED BY AN EXECUTIVE DIRECTOR, WHO SHALL BE APPOINTED BY THE SECRETARY OF THE DICT UPON THE RECOMMENDATION OF THE CIPC. THE EXECUTIVE DIRECTOR MUST HAVE ADEQUATE KNOWLEDGE ON, TRAINING AND EXPERIENCE IN THE PHENOMENON OF AND ISSUES INVOLVED IN CYBERSECURITY AND/OR CYBERCRIME AND IN THE FIELD OF LAW OR LAW ENFORCEMENT.

THE EXECUTIVE DIRECTOR SHALL BE UNDER THE SUPERVISION OF THE CIPC THROUGH ITS CHAIRPERSON

AND CO-CHAIRPERSONS, AND SHALL PERFORM THE FOLLOWING FUNCTIONS:

A. ACT AS SECRETARY OF THE CIPC AND ADMINISTRATIVE OFFICER OF ITS SECRETARIAT;
B. ADVISE AND ASSIST THE CHAIRPERSON AND CO-CHAIRPERSONS IN FORMULATING AND IMPLEMENTING THE OBJECTIVES, POLICIES, PLANS AND PROGRAMS OF THE CIPC, INCLUDING THOSE INVOLVING MOBILIZATION OF GOVERNMENT OFFICES REPRESENTED IN THE CIPC, AS WELL AS OTHER RELEVANT GOVERNMENT OFFICES, TASK FORCES, AND MECHANISMS;
C. SERVE AS PRINCIPAL ASSISTANT TO THE CHAIRPERSON AND CO-CHAIRPERSONS IN THE OVERALL SUPERVISION OF THE CIPC ADMINISTRATIVE BUSINESS;
D. OVERSEE ALL CIPC OPERATIONAL ACTIVITIES;
E. ENSURE AND EFFECTIVE AND EFFICIENT PERFORMANCE OF CIPC FUNCTIONS AND PROMPT IMPLEMENTATION OF CIPC OBJECTIVES, POLICIES, PLANS AND PROGRAMS;
F. PROPOSE EFFECTIVE ALLOCATIONS OF RESOURCES FOR IMPLEMENTING CIPC OBJECTIVES, POLICIES, PLANS AND PROGRAMS;
G. SUBMIT PERIODIC REPORTS TO THE CIPC ON THE PROGRESS OF CIPC OBJECTIVES, POLICIES, PLANS AND PROGRAMS;
H. PREPARE ANNUAL REPORTS OF ALL CIPC ACTIVITIES; AND
I. PERFORM OTHER DUTIES AS THE CIPC MAY ASSIGN."

SECTION 13. Section 26 of the same Act is hereby amended to read as follows:

"SEC. 26. *Powers and Functions.* – The [CICC] CIPC shall have the following powers and functions:

[(a) To formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);

(b) To coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in this Act;

(c) To monitor cybercrime cases being bandied by participating law enforcement and prosecution agencies;

(d) To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;

(e) To coordinate the support and participation of the business sector, local government units and nongovernment organizations in cybercrime prevention programs and other related projects;

(f) To recommend the enactment of appropriate laws, issuances, measures and policies;

(g) To call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions; and

(h) To perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as may be necessary for the proper implementation of this Act.]

A. COORDINATE THE PROGRAMS AND PROJECTS OF THE VARIOUS MEMBER AGENCIES TO EFFECTIVELY ADDRESS THE ISSUES AND PROBLEMS ATTENDANT TO CYBERSECURITY;

B. CONDUCT AND COORDINATE MASSIVE INFORMATION DISSEMINATIONS AND CAMPAIGN ON THE EXISTENCE OF THE LAW AND THE VARIOUS ISSUES AND PROBLEMS ATTENDANT TO CYBERSECURITY;

C. DIRECT OTHER AGENCIES TO IMMEDIATELY RESPOND TO THE PROBLEMS BROUGHT TO THEIR ATTENTION AND REPORT TO THE CIPC ON THE ACTION TAKEN;

D. ASSIST IN FILING OF CASES AGAINST INDIVIDUALS, AGENCIES, INSTITUTIONS OR ESTABLISHMENTS THAT VIOLATE THE PROVISIONS OF THIS ACT;

E. SECURE FROM ANY DEPARTMENT, BUREAU, OFFICE, AGENCY, OR INSTRUMENTALITY OF THE GOVERNMENT OR FROM NGOS AND OTHER CIVIC ORGANIZATIONS SUCH ASSISTANCE AS MAY BE NEEDED TO EFFECTIVELY IMPLEMENT THIS ACT;

F. ASSESS THE VULNERABILITIES OF THE COUNTRY'S CYBERSECURITY;

G. ISSUE UPDATED SECURITY PROTOCOLS TO ALL GOVERNMENT EMPLOYEES IN THE STORAGE, HANDLING AND DISTRIBUTION OF ALL FORMS (DIGITAL, ELECTRONIC, SNAIL MAIL, ETC.) OF DOCUMENTS AND COMMUNICATIONS. FOLLOWING BEST PRACTICES, THESE PROTOCOLS SHALL BE UPDATED PERIODICALLY AND AS NECESSARY, IN LIGHT OF THE RAPID DEVELOPMENTS IN INFORMATION AND COMMUNICATIONS TECHNOLOGY;

H. ENHANCE THE PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF INFORMATION SHARING INVOLVING CYBERATTACKS, THREATS AND VULNERABILITIES TO CYBER THREATS;

I. CONDUCT PERIODIC STRATEGIC PLANNING AND WORKSHOP ACTIVITIES THAT WILL REDUCE THE COUNTRY'S VULNERABILITIES TO CYBER THREATS;

J. DIRECT ITS MEMBER AGENCIES AND APPROPRIATE AGENCIES TO IMPLEMENT CYBERSECURITY MEASURES AS MAY BE REQUIRED BY THE SITUATION;

K. MAKE SUCH RECOMMENDATIONS AND/OR SUCH OTHER REPORTS AS THE PRESIDENT MAY FROM TIME TO TIME DIRECT; AND

L. EXERCISE ALL THE POWERS AND PERFORM SUCH OTHER FUNCTIONS NECESSARY TO ATTAIN THE PURPOSES AND OBJECTIVES OF THIS ACT."

SECTION 14. Section 28 of the same Act is hereby amended to read as follows:

"SEC. 28. *Implementing Rules and Regulations.* – The [ICTO-DOST, the] DOJ, DICT, and the Department of the Interior and Local Government (DILG) shall jointly formulate the necessary rules and regulations within ninety (90) days from approval of this Act, for its effective implementation."

SECTION 15. ***Separability Clause.*** – If any provision of this Act is declared unconstitutional, the same shall not affect the validity and effectivity of the other provisions hereof.

SECTION 16. ***Repealing Clause.*** – All laws, decrees, orders, and issuances or portions thereof, which are inconsistent with any of the provisions of this Act are hereby repealed, amended or modified accordingly. SECTION 4(C)(4) OF THE CYBERCRIME PREVENTION ACT OF 2012 AND Section 33(a) of Republic Act No. 8792 or the "Electronic Commerce Act" are hereby [modified accordingly] repealed.

SECTION 17. ***Effectivity.*** – This Act shall take effect fifteen (15) days after its complete publication in the Official Gazette or in at least two (2) national newspapers of general circulation.

Approved,