

SEVENTEENTH CONGRESS |
OF THE REPUBLIC OF THE PHILIPPINES |
Second Regular Session |

HOUSE OF REPRESENTATIVES

House Bill No. **6184**



Introduced by Representative Victor A. Yap

EXPLANATORY NOTE

Technological advancements move at an exponential pace. The internet platform we had 5 years ago is already outdated, if not obsolete. The World Wide Web is evolving at an unprecedented rate.

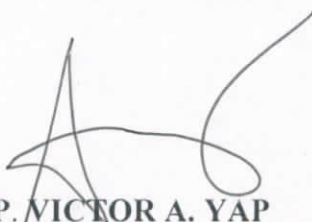
With these advancements, potential criminals are provided with more avenues to exploit technology for their nefarious deeds. Just recently, major companies in the world were subjected to cyber-attacks and were held ransom for the access of their database. These attacks could cripple an entire industry and adversely affect the economy of a country.

These events prompt us to further improve our anti-cyber crime law. Our law enforcement agencies must be equipped with the proper power and authority to deal with any cyber-attacks that may be directed against our citizens.

In the 2016-2017 Philippine Cybercrime report, the NBI Cybercrime Division and PNP Anti Cyber crime group received a total of 3,951 complaints and cyber-related offenses in 2016. This is more than 50% higher than the number of complaints received in 2015 which only totaled 2,567. We can only expect this number to rise as people are becoming more and more dependent on the internet.

This bill intends to empower the law enforcement agencies by mandating the PNP, the NBI and the DOJ to create their own cyber-crime divisions to ensure the strict implementation of the anti-cyber crime law. It also provides law enforcement agencies with the legal authority to intercept and collect computer data upon securing a court warrant. Ultimately, this bill seeks to attune our anti-cyber crime law to the technology of today.

In the interest of our people's security and safety, support for the passage and approval of this legislation is earnestly sought.


REP. VICTOR A. YAP
Second District, Province of Tarlac

HOUSE OF REPRESENTATIVES

House Bill No. **6184**

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.”

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

2
3 “SEC. 8-A. TEMPORARY DISQUALIFICATION TO ACCESS THE
4 INTERNET. – IN ADDITION TO THE IMPOSABLE IMPRISONMENT
5 AND/OR FINE MENTIONED IN THE IMMEDIATELY PRECEDING
6 SECTION, ANY PERSON FOUND GUILTY OF ANY OF THE
7 PUNISHABLE ACTS ENUMERATED IN THIS ACT SHALL BE
8 DEPRIVED THE RIGHT TO ACCESS THE INTERNET.

9
10 THE RIGHT OF THE ACCUSED OF ANY OF THE PUNISHABLE
11 ACTS HEREIN TO ACCESS THE INTERNET MAY BE SUSPENDED OR
12 LIMITED BY THE CYBERCRIME COURT PENDING FINAL JUDGMENT
13 UPON SHOWING, WITH DUE NOTICE AND HEARING, THAT THERE
14 IS A STRONG LIKELIHOOD THAT THE ACCUSED WILL BE ABLE TO
15 FACILITATE THE COMMISSION OF THE OFFENSE SO CHARGED
16 UNLESS SUCH ORDER WAS ISSUED.

17
18 THE SUSPENSION OF THE RIGHT TO ACCESS THE INTERNET
19 SHALL LAST DURING THE TERM OF THE SENTENCE OF THE
20 CONVICT.”

21
22 **SECTION 3.** Section 10 of the same Act is hereby amended to read as follows:

23
24 “SEC. 10. *[Law] Enforcement Authorities.* – [The National Bureau of Investigation (NBI)
25 and the Philippine National Police (PNP) shall be responsible for the efficient and effective
26 law enforcement of the provisions of this Act. The NBI and the PNP shall organize a
27 cybercrime unit or center manned by special investigators to exclusively handle cases
28 involving violations] THERE IS HEREBY CREATED AN ANTI-CYBERCRIME
29 GROUP IN THE PHILIPPINE NATIONAL POLICE (PNP), A CYBERCRIME
30 DIVISION IN THE NATIONAL BUREAU OF INVESTIGATION (NBI), AND AN
31 OFFICE OF CYBERCRIME WITHIN THE DEPARTMENT OF JUSTICE (DOJ) TO
32 IMPLEMENT THE PROVISIONS of this Act.”

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

34
35 “SEC. 11. *DUTIES AND FUNCTIONS OF THE PNP-ANTI-CYBERCRIME*
36 *GROUP AND THE NBI CYBERCRIME DIVISION.* [Duties of Law
37 Enforcement Authorities.] — [To ensure that the technical nature of
38 cybercrime and its prevention is given focus and considering the procedures
39 involved for international cooperation, law enforcement authorities specifically

1 the computer or technology crime divisions or units responsible for the
2 investigation of cybercrimes are required to submit timely and regular reports
3 including pre-operation, post-operation and investigation results and such other
4 documents as may be required to the Department of Justice (DOJ) for review
5 and monitoring.] THE PNP ANTI-CYBERCRIME GROUP AND THE NBI
6 CYBERCRIME DIVISION SHALL HAVE THE FOLLOWING DUTIES
7 AND FUNCTIONS:

8
9 (A) TO INVESTIGATE THE PROHIBITED ACTS UNDER
10 CHAPTER II AND TO SUPPORT INVESTIGATIONS WHERE
11 COMPUTER SYSTEMS ARE INVOLVED INCLUDING THE
12 SEARCH, SEIZURE, EVIDENCE PRESERVATION,
13 FORENSIC RECOVERY OF DATA FROM CRIME SCENES
14 AND SYSTEMS USED IN CRIMES;

15
16 (B) TO CONDUCT DATA RECOVERY AND FORENSIC
17 ANALYSIS ON COMPUTER SYSTEMS AND OTHER
18 ELECTRONIC EVIDENCE SEIZED AS PROVIDED UNDER
19 CHAPTER IV OF THIS ACT;

20
21 (C) TO FORMULATE GUIDELINES IN INVESTIGATION,
22 FORENSIC EVIDENCE RECOVERY, AND FORENSIC
23 DATA ANALYSIS CONSISTENT WITH INDUSTRY
24 STANDARD AND INTERNATIONAL BEST PRACTICES;

25
26 (D) TO DEVELOP CAPACITY WITHIN THEIR
27 ORGANIZATIONS INCLUDING EXTENDING TECHNICAL
28 SUPPORT AND TO PERFORM SUCH DUTIES NECESSARY
29 FOR THE ENFORCEMENT OF THIS ACT; AND

30
31 (E) TO MAINTAIN DATABASE OF THE COMPLAINTS
32 RECEIVED AND SUBMIT TIMELY AND REGULAR
33 REPORTS PERTAINING THERETO, INCLUDING PRE-
34 OPERATION, POST-OPERATION AND INVESTIGATION
35 RESULTS, AND SUCH OTHER DOCUMENTS AS MAY BE
36 REQUIRED TO THE DOJ – OFFICE OF CYBERCRIME FOR
37 REVIEW AND MONITORING, TO ENSURE THAT THE
38 TECHNICAL NATURE OF CYBERCRIME AND ITS
39 PREVENTION IS GIVEN FOCUS AND CONSIDERING THE

1 PROCEDURES INVOLVED FOR INTERNATIONAL
2 COOPERATION.
3

4 THE PNP ANTI-CYBERCRIME GROUP AND THE NBI
5 CYBERCRIME DIVISION SHALL RESPECTIVELY BE HEADED BY AT
6 LEAST A POLICE DIRECTOR (2-STAR RANK) AND A DIRECTOR II.”
7

8 **SECTION 5.** New sections shall be inserted after Section 11 to read as follows:
9

10 “SEC. 11-A. *CYBERCRIME INVESTIGATION.* – ALL
11 CYBERCRIME INVESTIGATIONS SHALL BE COORDINATED WITH
12 THE DOJ – OFFICE OF CYBERCRIME. DURING CYBERCRIME
13 INVESTIGATIONS, THE DOJ – OFFICE OF CYBERCRIME SHALL ACT
14 AS A COMPETENT AUTHORITY FOR ALL REQUESTS FOR
15 ASSISTANCE FOR INVESTIGATION OR PROCEEDINGS
16 CONCERNING CYBERCRIMES, INCLUDING THE PROVISION OF
17 LEGAL AND/OR TECHNICAL ADVICE.
18

19 SEC. 11-B. *INVESTIGATING PROSECUTORS IN CYBERCRIME*
20 *INVESTIGATIONS.* – THERE SHALL BE SPECIALLY TRAINED
21 PROSECUTORS FROM THE DOJ NATIONAL PROSECUTION SERVICE
22 ASSIGNED TO THE DOJ – OFFICE OF CYBERCRIME TO DIRECTLY
23 CONTROL AND SUPERVISE CYBERCRIME INVESTIGATIONS.
24

25 LAW ENFORCERS SHALL TAKE GUIDANCE FROM, AND
26 COOPERATE CLOSELY, WITH THE INVESTIGATING PROSECUTOR
27 IN THE PROCESS OF CONDUCTING CYBERCRIME INVESTIGATIONS,
28 ESPECIALLY IN MATTERS CONCERNING COMPLIANCE WITH LAWS
29 AND RULES OF PROCEDURE, EVIDENCE-GATHERING, AND CASE-
30 BUILD UP AND OPERATIONS.
31

32 SEC. 11-C. *POWERS OF THE INVESTIGATING PROSECUTOR*
33 *DURING CYBERCRIME INVESTIGATIONS.* – THE INVESTIGATING
34 PROSECUTOR SHALL EXERCISE THE FOLLOWING POWERS
35 DURING CYBERCRIME INVESTIGATIONS:
36

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

- 1
- 2 (B) PERFORM ALL ACTS NECESSARY TO ENSURE THE
- 3 INTEGRITY OF THE CYBERCRIME INVESTIGATION
- 4 PROCESS AND ITS COMPLIANCE WITH RELEVANT
- 5 LAWS AND RULES;
- 6
- 7 (C) ENSURE THE INTEGRITY OF THE CHAIN OF CUSTODY
- 8 OVER EVIDENCE AT ALL STAGES OF THE CYBERCRIME
- 9 INVESTIGATION;
- 10
- 11 (D) CAUSE THE APPLICATION FOR COURT WARRANTS FOR
- 12 SEARCH, SEIZURE, EXAMINATION, INTERCEPTION AND
- 13 COLLECTION, AND DISCLOSURE OF COMPUTER DATA,
- 14 AND SUCH OTHER PROCESSES AS MAY BE NECESSARY
- 15 IN THE COURSE OF THE CYBERCRIME INVESTIGATION;
- 16 AND
- 17
- 18 (E) DIRECT LAW ENFORCERS TO SUBMIT INVENTORIES,
- 19 REPORTS, FINDINGS AND OTHER DOCUMENTS, AS MAY
- 20 BE REQUIRED, IN CONNECTION WITH THE
- 21 CYBERCRIME INVESTIGATION.
- 22

23 THE FOREGOING NOTWITHSTANDING, NO INVESTIGATING

24 PROSECUTOR SHALL FORM PART OF THE DOJ PROSECUTION TASK

25 FORCE ON CYBERCRIME WHOSE PRIMARY DUTY CONSISTS OF

26 DETERMINING PROBABLE CAUSE, AND THE PROSECUTION OF THE

27 OFFENDERS, IN CYBERCRIME AND CYBER-RELATED CASES.”

28

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

30

31 “SEC 12. INTERCEPTION AND COLLECTION OF COMPUTER

32 DATA. [Real-Time Collection of Traffic Data. – Law enforcement authorities,

33 with due cause, shall be authorized to collect or record by technical or electronic

34 means traffic data in real-time associated with specified communications

35 transmitted by means of a computer system.

36 Traffic data refer only to the communication’s origin, destination, route,

37 time, date, size, duration, or type of underlying service, but not content, nor

38 identities.

1 All other data to be collected or seized or disclosed will require a court
2 warrant.

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

5 The court warrant required under this section shall only be issued or
6 granted upon written application and the examination under oath or affirmation
7 of the applicant and the witnesses he may produce and the showing: (1) that there
8 are reasonable grounds to believe that any of the crimes enumerated hereinabove
9 has been committed, or is being committed, or is about to be committed: (2) that
10 there are reasonable grounds to believe that evidence that will be obtained is
11 essential to the conviction of any person for, or to the solution of, or to the
12 prevention of, any such crimes; and (3) that there are no other means readily
13 available for obtaining such evidence.]
14

15 LAW ENFORCEMENT AUTHORITIES SHALL, UPON SECURING
16 A COURT WARRANT, BE AUTHORIZED TO CONDUCT INTERCEPTION
17 AND/OR COLLECTION OF TRAFFIC AND CONTENT DATA.
18

19 THIS ALSO APPLIES TO THE CONDUCT OF INTERCEPTION
20 AND/OR COLLECTION BY LAW ENFORCEMENT AUTHORITIES OF
21 TRAFFIC AND CONTENT DATA THAT IS HELD OR MAINTAINED BY A
22 CLOUD COMPUTING SERVICE PROVIDER SITUATED OUTSIDE THE
23 PHILIPPINES EITHER:
24

25 (A) ON BEHALF OF, AND RECEIVED BY MEANS OF ELECTRONIC
26 TRANSMISSION FROM OR CREATED BY MEANS OF
27 COMPUTER PROCESSING OF COMMUNICATIONS RECEIVED
28 BY MEANS OF ELECTRONIC TRANSMISSION FROM, A
29 SUBSCRIBER OR CUSTOMER OF SUCH CLOUD COMPUTING
30 SERVICE; AND
31

32 (B) SOLELY FOR THE PURPOSE OF PROVIDING STORAGE OR
33 COMPUTER PROCESSING SERVICES TO SUCH SUBSCRIBER
34 OR CUSTOMER, IF THE PROVIDER IS NOT AUTHORIZED TO
35 ACCESS THE CONTENTS OF ANY SUCH COMMUNICATIONS
36 FOR PURPOSES OF PROVIDING ANY SERVICES OTHER THAN
37 STORAGE OR COMPUTER PROCESSING.
38

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

5
6 SERVICE PROVIDERS ARE REQUIRED TO COOPERATE AND
7 ASSIST LAW ENFORCEMENT AUTHORITIES IN THE COLLECTION OR
8 RECORDING OF THE ABOVE-STATED INFORMATION.

9
10 THE FOREGOING NOTWITHSTANDING, ANY ENFORCEMENT
11 AUTHORITY OR ANY PERSON, WHO IS A PARTY TO A
12 COMMUNICATION SUBJECT OF A SPECIFIED COMPUTER DATA, MAY
13 GIVE HIS CONSENT TO AND/OR AUTHORIZE SUCH INTERCEPTION
14 AND COLLECTION, AND MAY REQUIRE THE PERSON OR SERVICE
15 PROVIDER TO COLLECT OR RECORD BY TECHNICAL OR
16 ELECTRONIC MEANS THE NECESSARY DATA AND/OR TO
17 COOPERATE OR ASSIST IN THE COLLECTION OR RECORDING OF
18 COMPUTER DATA.

19
20 IN ALL INSTANCES, IT SHALL BE ENSURED THAT THE DATA
21 TO BE COLLECTED OR RECORDED SHALL BE LIMITED EITHER TO
22 THE DATA DESCRIBED IN THE COURT WARRANT OR TO THE
23 SPECIFIED COMMUNICATION TO WHICH THEY ARE A PARTY TO.”

24
25 **SECTION 7.** Section 15 of the same Act is hereby amended to read as follows:

26
27 “SEC. 15. *Search, seizure, and examination of computer data.* – Where a search
28 and seizure warrant is properly issued, the [law] enforcement authorities shall
29 likewise have the following powers and duties:

30
31 Within the time period specified in the warrant, to conduct interception,
32 as defined in this Act, and:

33
34 (A) SEARCH AND SEIZE COMPUTER DATA SUBJECT OF
35 THE COURT WARRANT;

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

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

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

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

6 [(e)](F) [To] R[r]ender inaccessible or remove those computer data in the
7 accessed computer or computer and communications network.
8

9 Pursuant thereof, enforcement authorities may order any person who [has]
10 MAY HAVE knowledge of the functioning of the computer system [and the measures
11 to protect and preserve the computer data therein to provide, as is reasonable, the
12 necessary information, to enable the undertaking of] TO ASSIST IN the search, seizure
13 and examination.

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

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

31 WITHIN FORTY-EIGHT (48) HOURS AFTER THE EXPIRATION OF THE
32 PERIOD GRANTED BY THE COURT UNDER THE IMMEDIATELY PRECEDING
33 PARAGRAPH, ENFORCEMENT AUTHORITIES SHALL FORTHWITH MAKE
34 THE FULL RETURN OF THE WARRANT AND DEPOSIT WITH THE COURT
35 ALL COMPUTER DATA EXAMINED. THE COURT SHALL ASCERTAIN THAT
36 THE HASH VALUES SUBMITTED DURING THE INITIAL RETURN AND THE
37 FULL RETURN ARE THE SAME AND INTACT TO ENSURE THE INTEGRITY
38 OF EVIDENCE WERE PRESERVED.”
39

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

2
3 “SEC. 23. DOJ-Office of Cybercrime. – [There is hereby created an Office of
4 Cybercrime within the DOJ designated as the central authority in all matters related to
5 international mutual assistance and extradition.] THE DOJ – OFFICE OF
6 CYBERCRIME SHALL HAVE THE FOLLOWING DUTIES AND FUNCTIONS:

7
8 (A) SERVE AS THE CENTRAL AUTHORITY IN ALL MATTERS
9 RELATED TO INTERNATIONAL MUTUAL ASSISTANCE
10 AND EXTRADITION FOR CYBERCRIME AND CYBER-
11 RELATED CASES, INCLUDING SENDING AND
12 ANSWERING REQUESTS FOR MUTUAL ASSISTANCE, THE
13 EXECUTION OF SUCH REQUESTS OR THEIR
14 TRANSMISSION TO THE AUTHORITIES COMPETENT FOR
15 THEIR EXECUTION;

16
17 (B) ACT AS THE PRINCIPAL ADMINISTRATOR AND FOCAL
18 AUTHORITY OF THIS ACT, INCLUDING FORMULATING
19 AND IMPLEMENTING LAW ENFORCEMENT
20 INVESTIGATION AND PROSECUTION STRATEGIES IN
21 CURBING CYBERCRIME AND CYBER-RELATED CASES TO
22 ENSURE THAT THE TECHNICAL NATURE OF
23 CYBERCRIME AND ITS PREVENTION IS GIVEN FOCUS
24 AND CONSIDERING THE PROCEDURES FOR
25 INTERNATIONAL COOPERATION;

26
27 (C) ISSUE PRESERVATION ORDERS ADDRESSED TO SERVICE
28 PROVIDERS;

29
30 (D) ADMINISTER OATHS, ISSUE SUBPOENA AND SUMMON
31 WITNESSES TO APPEAR IN AN INVESTIGATION OR
32 PROCEEDINGS FOR CYBERCRIME;

33
34 (E) REQUIRE THE SUBMISSION OF TIMELY AND REGULAR
35 REPORTS INCLUDING PRE-OPERATION, POST-
36 OPERATION AND INVESTIGATION RESULTS, AND SUCH
37 OTHER DOCUMENTS FROM THE PNP AND NBI FOR
38 MONITORING AND REVIEW;

- 1 (F) MONITOR THE COMPLIANCE OF THE SERVICE
2 PROVIDERS WITH THE PROVISIONS OF CHAPTER IV OF
3 THIS ACT;
4
- 5 (G) FACILITATE INTERNATIONAL COOPERATION WITH
6 OTHER AGENCIES ON INTELLIGENCE, TRAINING, AND
7 CAPACITY-BUILDING RELATED TO CYBERCRIME
8 PREVENTION, SUPPRESSION, INVESTIGATION AND
9 PROSECUTION;
10
- 11 (H) ISSUE AND PROMULGATE GUIDELINES, ADVISORIES,
12 AND PROCEDURES IN ALL MATTERS RELATED TO
13 CYBERCRIME INVESTIGATION, FORENSIC EVIDENCE
14 RECOVERY, AND FORENSIC DATA ANALYSIS
15 CONSISTENT WITH INDUSTRY STANDARD PRACTICES;
16
- 17 (I) PRESCRIBE FORMS AND TEMPLATES, INCLUDING, BUT
18 NOT LIMITED TO, THOSE FOR PRESERVATION ORDERS,
19 CHAIN OF CUSTODY, CONSENT TO SEARCH, CONSENT TO
20 ASSUME ACCOUNT/ONLINE IDENTITY, AND REQUEST
21 FOR COMPUTER FORENSIC EXAMINATION; AND
22
- 23 (J) PERFORM SUCH OTHER ACTS NECESSARY FOR THE
24 IMPLEMENTATION OF THIS ACT.”
25

26 **SECTION 9.** A new section shall be inserted after Section 23 to read as follows:
27

28 “SEC. 23-A. *NATIONAL COMPUTER FORENSICS TRAINING*
29 *PROGRAM.* – IN RELATION TO SECTION 23 (B) OF THIS ACT, THERE IS
30 HEREBY ESTABLISHED A NATIONAL COMPUTER FORENSICS
31 TRAINING PROGRAM (NCFTP) UNDER THE MANAGEMENT AND
32 SUPERVISION OF THE DOJ – OFFICE OF CYBERCRIME, WHICH SHALL
33 PROVIDE FOR A CONSOLIDATED TRAINING IN COMPUTER
34 FORENSICS AMONG ALL LAW ENFORCEMENT AGENCIES,
35 CONSISTENT WITH INTERNATIONAL BEST PRACTICES.
36

37 THE AMOUNT OF FIFTY MILLION PESOS (PHP50,000,000.00)
38 NECESSARY FOR THE IMPLEMENTATION OF THIS PROGRAM SHALL

1 BE APPROPRIATED ANNUALLY IN THE GENERAL APPROPRIATIONS
2 ACT OF DOJ.”
3

4 **SECTION 10.** Section 24 of the same Act is hereby amended to read as follows:
5

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

18 **SECTION 11.** Section 25 of the same Act is hereby amended to read as follows:
19

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

- 33
34 A. SECRETARY, DEPARTMENT OF FOREIGN AFFAIRS;
35 B. SECRETARY, DEPARTMENT OF ENERGY;
36 C. SECRETARY, DEPARTMENT OF FINANCE;
37 D. SECRETARY, DEPARTMENT OF THE INTERIOR AND
38 LOCAL GOVERNMENT (DILG);

- 1 E. SECRETARY, DEPARTMENT OF SCIENCE AND
2 TECHNOLOGY;
3 F. SECRETARY, DEPARTMENT OF NATIONAL DEFENSE;
4 G. SECRETARY, DEPARTMENT OF TRANSPORTATION;
5 H. SECRETARY, PRESIDENTIAL COMMUNICATIONS
6 OPERATION OFFICE;
7 I. CHAIRMAN, NATIONAL PRIVACY COMMISSION;
8 J. COMMISSIONER, NATIONAL TELECOMMUNICATIONS
9 COMMISSION;
10 K. EXECUTIVE DIRECTOR, ANTI-TERRORISM COUNCIL;
11 L. EXECUTIVE DIRECTOR, ANTI-MONEY LAUNDERING
12 COUNCIL;
13 M. EXECUTIVE DIRECTOR, PHILIPPINE CENTER ON
14 TRANSNATIONAL CRIME;
15 N. DIRECTOR GENERAL, PHILIPPINE NATIONAL POLICE;
16 O. DIRECTOR, NATIONAL BUREAU OF INVESTIGATION;
17 AND
18 P. ONE (1) REPRESENTATIVE EACH FROM THE PRIVATE
19 SECTOR, NON-GOVERNMENTAL ORGANIZATION, AND
20 ACADEME. THESE REPRESENTATIVES SHALL BE
21 NOMINATED BY THE GOVERNMENT AGENCY
22 REPRESENTATIVES OF THE CIPC FOR THE APPOINTMENT
23 BY THE PRESIDENT FOR A TERM OF THREE (3) YEARS.
24

25 THE MEMBERS OF THE CIPC MAY DESIGNATE THEIR
26 PERMANENT REPRESENTATIVES WHO SHALL HAVE A RANK NOT
27 LOWER THAN AN ASSISTANT SECRETARY OR ITS EQUIVALENT, TO
28 MEETINGS AND SHALL RECEIVE EMOLUMENTS AS MAY BE
29 DETERMINED BY THE CIPC IN ACCORDANCE WITH EXISTING
30 BUDGET AND ACCOUNTING RULES AND REGULATIONS.”
31

32 **SECTION 12.** A new section shall be inserted after Section 25 to read as follows:
33

34 “SEC. 25-A. *SECRETARIAT TO THE CIPC.* – THE DICT SHALL
35 ESTABLISH THE NECESSARY SECRETARIAT FOR THE CIPC WHICH
36 SHALL PROVIDE SUPPORT FOR THE FUNCTIONS AND PROJECTS OF
37 THE CIPC.
38

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

8
9 THE EXECUTIVE DIRECTOR SHALL BE UNDER THE
10 SUPERVISION OF THE CIPC THROUGH ITS CHAIRPERSON AND CO-
11 CHAIRPERSONS, AND SHALL PERFORM THE FOLLOWING
12 FUNCTIONS:

- 13
- 14 A. ACT AS SECRETARY OF THE CIPC AND ADMINISTRATIVE
15 OFFICER OF ITS SECRETARIAT;
 - 16 B. ADVISE AND ASSIST THE CHAIRPERSON AND CO-
17 CHAIRPERSONS IN FORMULATING AND IMPLEMENTING
18 THE OBJECTIVES, POLICIES, PLANS AND PROGRAMS OF
19 THE CIPC, INCLUDING THOSE INVOLVING
20 MOBILIZATION OF GOVERNMENT OFFICES
21 REPRESENTED IN THE CIPC, AS WELL AS OTHER
22 RELEVANT GOVERNMENT OFFICES, TASK FORCES, AND
23 MECHANISMS;
 - 24 C. SERVE AS PRINCIPAL ASSISTANT TO THE CHAIRPERSON
25 AND CO-CHAIRPERSONS IN THE OVERALL SUPERVISION
26 OF THE CIPC ADMINISTRATIVE BUSINESS;
 - 27 D. OVERSEE ALL CIPC OPERATIONAL ACTIVITIES;
 - 28 E. ENSURE AND EFFECTIVE AND EFFICIENT PERFORMANCE
29 OF CIPC FUNCTIONS AND PROMPT IMPLEMENTATION OF
30 CIPC OBJECTIVES, POLICIES, PLANS AND PROGRAMS;
 - 31 F. PROPOSE EFFECTIVE ALLOCATIONS OF RESOURCES FOR
32 IMPLEMENTING CIPC OBJECTIVES, POLICIES, PLANS AND
33 PROGRAMS;
 - 34 G. SUBMIT PERIODIC REPORTS TO THE CIPC ON THE
35 PROGRESS OF CIPC OBJECTIVES, POLICIES, PLANS AND
36 PROGRAMS;
 - 37 H. PREPARE ANNUAL REPORTS OF ALL CIPC ACTIVITIES;
38 AND
 - 39 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;

- 1 E. SECURE FROM ANY DEPARTMENT, BUREAU, OFFICE,
2 AGENCY, OR INSTRUMENTALITY OF THE GOVERNMENT
3 OR FROM NGOS AND OTHER CIVIC ORGANIZATIONS
4 SUCH ASSISTANCE AS MAY BE NEEDED TO EFFECTIVELY
5 IMPLEMENT THIS ACT;
- 6 F. ASSESS THE VULNERABILITIES OF THE COUNTRY'S
7 CYBERSECURITY;
- 8 G. ISSUE UPDATED SECURITY PROTOCOLS TO ALL
9 GOVERNMENT EMPLOYEES IN THE STORAGE,
10 HANDLING AND DISTRIBUTION OF ALL FORMS (DIGITAL,
11 ELECTRONIC, SNAIL MAIL, ETC.) OF DOCUMENTS AND
12 COMMUNICATIONS. FOLLOWING BEST PRACTICES,
13 THESE PROTOCOLS SHALL BE UPDATED PERIODICALLY
14 AND AS NECESSARY, IN LIGHT OF THE RAPID
15 DEVELOPMENTS IN INFORMATION AND
16 COMMUNICATIONS TECHNOLOGY;
- 17 H. ENHANCE THE PUBLIC-PRIVATE PARTNERSHIP IN THE
18 FIELD OF INFORMATION SHARING INVOLVING
19 CYBERATTACKS, THREATS AND VULNERABILITIES TO
20 CYBER THREATS;
- 21 I. CONDUCT PERIODIC STRATEGIC PLANNING AND
22 WORKSHOP ACTIVITIES THAT WILL REDUCE THE
23 COUNTRY'S VULNERABILITIES TO CYBER THREATS;
- 24 J. DIRECT ITS MEMBER AGENCIES AND APPROPRIATE
25 AGENCIES TO IMPLEMENT CYBERSECURITY MEASURES
26 AS MAY BE REQUIRED BY THE SITUATION;
- 27 K. MAKE SUCH RECOMMENDATIONS AND/OR SUCH OTHER
28 REPORTS AS THE PRESIDENT MAY FROM TIME TO TIME
29 DIRECT; AND
- 30 L. EXERCISE ALL THE POWERS AND PERFORM SUCH OTHER
31 FUNCTIONS NECESSARY TO ATTAIN THE PURPOSES AND
32 OBJECTIVES OF THIS ACT."
- 33

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

35

36 "SEC. 28. *Implementing Rules and Regulations.* – The [ICTO-DOST, the] DOJ,
37 DICT, and the Department of the Interior and Local Government (DILG) shall jointly
38 formulate the necessary rules and regulations within ninety (90) days from approval of this
39 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,