



Republic of the Philippines
Department of Education
REGION I



Advisory No. 144, s. 2021
October 19, 2021

In compliance with DepEd Order (D.O) No. 8, s. 2013
this advisory is issued not for endorsement per D.O No. 28, s. 2001,
but only for the information of DepEd Officials,
personnel/staff, as well as the concerned public.
(Visit www.deped.gov.ph)

**INVITATION TO ATTEND TO AN ONLINE WORKSHOP FOR BREACH RESPONSE
AND CYBER SECURITY**

The Yisrael Solutions and Training Center, Inc. is offering an Online Workshop
for Breach Response and Cyber Security on a tentative schedule: October 25-27,
November 22-24 and December 20-22, 2021.

Personnel who have access to private data and information of persons of the
schools division offices and public and private elementary and secondary schools are
invited to participate on a voluntary basis.

Participation of public and private schools shall be subject to the no-disruption-
of-classes policy stipulated in DepEd Order No. 9, s. 2005 entitled Instituting
Measures to Increase Engaged Time-on-Task and Ensuring Compliance Therewith.

Attached is the copy of the invitation for information.

For queries and confirmation of attendance, kindly contact:

Nharis A. Aspacio

Focal Person

Email: nharis.aspacio@yisrael-dataprivacy.com

Mobile No.: 09661877756/09171157990/09614767056

Landline: (632) 616-3086

Telefax: (02) 956-2025

flay for privs.

ORD-LU/RMW/gsl/ADV005
October 19, 2021



DepEd RO1 LEGAL 210703

DepEd Region 1: Built on character; empowered by competence.



Flores St., Catbangan, City of San Fernando, La Union
(072) 607-8137 / 682-2324
region1@deped.gov.ph | www.depedro1.com





TOLENTINO G. AQUINO

Director III

Department of Education-Regional Office 1

Tel/Fax no: (072) 607-8143 / 607-8136TF/ 607-8137

region1@deped.gov.ph, action@deped.gov.ph

SUBJECT: "INVITATION TO ATTEND TO AN ONLINE WORKSHOP FOR BREACH RESPONSE AND CYBER SECURITY"

Dear Sir/Madam,

Greetings!

Yisrael Solutions and Training Center Inc is committed for the welfare of the country and the people. In line with the recent pandemic or the amid spread of COVID 19, the conduct of training classes or seminar/workshops all over the country had been temporarily postponed indefinitely until further notice to ensure the security, health and safety of our countrymen. However, we have decided to continue our operations with virtual classrooms and remote work through the use of digital communication technology.

As an alternative option for face-to-face, we would like to offer you our online workshop, the online equivalent of being in a training room and learning together as a group through collaborative activities which will be conducted over the internet.

Cyber security awareness training is essential to reduce the risk that employees exposed and tricked by sophisticated phishing or social engineering methods into serving unknowingly as entry points or worst, breach incidents that can affect organization information and data systems. This training could also help the company/agency to respond in a security breach and comply with the necessary notification requirements under the Philippine Data Privacy Act.

The primary objective of the security awareness program is to educate users on their responsibility to help protect the confidentiality, availability and integrity of their organization's information and information assets. The participants will be able know the state-of-the art information about Cyber Security, it's importance, good practices and benefits to the organization. Participants can have a view on different phases of security threats: System Hacking, Malware Threat, Sniffing, Social Engineering, DDOS Attack and How can they respond to them.

During the training, the speakers will also confer on Breach simulation briefing and simulation of attack and a Breach Notification Requirements of RA 10173, a deep discussion on breach notification requirements under the DPA and Circular 16-03 and additional information on RA 10175 "Cybercrime Act"

Participants will take their time to report the results of their investigation on the given breach simulation, both technical and compliance report that is why we encourage you to form or create a Breach Response team (minimum number or three (3) or more participants) to be headed by the Data Protection Officer (DPO) to attend and participate on the "Breach Response Team Report.



Documan®

DepEd RO1

REC2114375



While we are staying at home to help controlling the spread of COVID 19, we are inviting you to attend in our online workshop classes for Breach Response and Cyber Security Threat and Attacks. Our cyber security expert will give discussion and demo about Cyber Threats and Attacks.

Below are the online workshop class programs/modules:

MODULE	TOPIC	TIME PERIOD	OBJECTIVES
1	DAY 1: INTRODUCTION TO CYBER SECURITY	9:00AM	Know the state-of-the art information about Cyber Security, it's importance, good practices and benefits to the organization
2	KNOWING THE ATTACK VECTORS (PART I)	TO 4:00PM	Participants can have a view on different phases of security threats: System Hacking, Malware Threat, Sniffing, Social Engineering, DDOS Attack and How can they respond to them.
3	DAY 2: KNOWING THE ATTACK VECTORS (PART II)	9:00AM	Continuation of discussion on phases of security threats: Hacking web servers, SQL Injection, Hacking Wireless Networks and Mobile Platforms
4	MANAGEMENT APPROACH: INCIDENT RESPONSE FRAMEWORK	TO 4:00PM	The session will provide guidance and additional information on security incident response framework
5	BREACH AND LIVE-ATTACK SIMULATION		Breach simulation briefing and simulation of attack
6	DAY 3: BREACH NOTIFICATION REQUIREMENTS OF RA 10173	9:00AM	A deep discussion on breach notification requirements under the DPA and Circular 16-03 and additional information on RA 10175 "Cybercrime Act"
7	BREACH RESPONSE TEAM REPORT (PRESENTATION OF REPORTS)	TO 4:00PM	Participants will take their time to report the results of their investigation on the given breach simulation, both technical and compliance report.

TENTATIVE WORKSHOP SCHEDULE:

October 25-27, 2021

November 22-24, 2021

December 20-22, 2021



Our online workshop will be held for three (3) days and the Online Workshop Fee is Php 1,800/day per pax (inclusive of tax). Kindly fill up the attached Confirmation Form which requires a list of your participants and email at nharis@yisraelsolutions.com for your workshop schedule. Please deposit the payment and email the deposit slip then a meeting ID and a password will be sent to your email. Payment should be made on the account of **YISRAEL SOLUTIONS & CONSULTING (YISCON) INC.**

We also conduct an in-house workshop wherein a central office can organize its regions to attend to on an online workshop. If you are interested, please inform us at the contact numbers stated below.

For inquiries and/or clarification, please contact us by email at nharis@yisraelsolutions.com (attention to: Nharis A. Aspacio); or thru text at mobile number 0966-1877-756-GLOBE; landline (632) 616-3086; telefax at (02) 956-2025.

Our team, though working from our own homes, would like to remind you to sanitize your gadgets, aside from washing hands frequently, as an added precautionary measure to prevent the spread of the virus.

We hope to see you in our online workshops!

YISRAEL SOLUTIONS AND TRAINING CENTER INC.

PRIVACY STATEMENT

We are committed to maintaining the accuracy, confidentiality, and security of your personally identifiable information ("Personal Information"). As part of this commitment, our privacy policy governs our actions as they relate to the collection, use and disclosure of Personal Information.

We are responsible for maintaining and protecting the Personal Information under our control. We have designated an individual or individuals who is/are responsible for compliance with our privacy policy.

Personal information will generally be collected directly from you through the use of any of our standard forms, over the internet, via email, or through a telephone conversation with you. We may also collect personal information about you from third parties acting on your behalf (for instance, agents or contact person).

We also collect information from subscribers (persons registering their details with us through the website) or website visitors for the purpose of improving our quality and effectiveness and to provide you with information. We will not publish your name in connection with any information you provide without your permission.



YISRAEL SOLUTIONS AND TRAINING CENTER, INC.

MESSAGE: Please fill-out the form below (**readable and correct name spelling of participants**)

CONFIRMATION FORM (CYBERSECURITY AWARENESS & BREACH RESPONSE)

(Please take note that Confirmation/Reservation is on First Come First Serve Basis)

Name of Company:			
Type of Organization:			Region:
Complete Address:			
Contact Person:	Tel. No.	Mobile No.	Fax No.

PARTICIPANT DETAILS:

First Name	M. I	Last Name	Mobile No.	Position	Email Address

Please reserve me/us on this workshop schedule:

SCHEDULE	Time	No. of Slot Reserve	REGISTRATION POLICY: GUARANTEED SLOTS Please fill up the confirmation form to guarantee your slots. Those who confirmed will be given "priority status" contingent upon availability of slots.
	9:00am -4:00p m		
Registration fee for 3-day workshop: (non-VAT) P 5,400			
Requested by: <hr/> Signature over printed Name		Pls deposit your payment to our LandBank Account BANK DETAILS: Account Name: YISRAEL SOLUTIONS & CONSULTING (YISCON) INC Account Number: 1641-1047-16 Pasig-C. Raymundo Ave. Branch	

PRIVACY NOTICE:

"We from Yisrael Solutions and Consulting (YISCON), Inc. will make sure that all of the personal information you have provided will be secured and remain confidential as much as possible. We collect information with your proper consent and that necessary personal in information with the intent to fulfil the purpose in transacting with us."

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth
day of July, two thousand eleven.



[REPUBLIC ACT NO. 10175]

AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE
PREVENTION, INVESTIGATION, SUPPRESSION AND
THE IMPOSITION OF PENALTIES THEREFOR AND
FOR OTHER PURPOSES

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

CHAPTER I

PRELIMINARY PROVISIONS

SECTION 1. *Title.* — This Act shall be known as the
“Cybercrime Prevention Act of 2012”.

SEC. 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.

SEC. 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.

(h) *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.

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

(j) *Critical infrastructure* refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

(k) *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.

(l) *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.

(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) *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; and

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

(o) *Subscriber's information* refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers 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.

(p) *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.

CHAPTER II

PUNISHABLE ACTS

SEC. 4. *Cybercrime Offenses.* — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

(1) *Illegal Access.* — The access to the whole or any part of a computer system without right.

(2) *Illegal Interception.* — The interception made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data.

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

(4) *System Interference.* — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

(5) *Misuse of Devices.* —

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

(aa) A device, 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, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

(ii) The possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this section.

(6) Cyber-squatting. – The acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and 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.

(b) Computer-related Offenses:

(1) Computer-related Forgery. –

(i) The input, alteration, or deletion of any computer 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 computer 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. – The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: *Provided*, That if no

damage has yet been caused, the penalty imposable shall be one (1) degree lower.

(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. – The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

(2) Child Pornography. – The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: *Provided*, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

(3) Unsolicited Commercial Communications. – The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:

(i) There is prior affirmative consent from the recipient;
or

(ii) The primary intent of the communication is for service and/or administrative announcements from the sender to its existing users, subscribers or customers; or

(iii) The following conditions are present:

(aa) The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages (opt-out) from the same source;

(bb) The commercial electronic communication does not purposely disguise the source of the electronic message; and

(cc) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

(4) 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.

SEC. 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 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.

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies 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.

SEC. 7. *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

SEC. 8. *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 (PhP200,000.00) 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 (PhP500,000.00) or both.

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed.

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 *prision 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 shall be punished with the penalties as enumerated in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty thousand pesos (PhP50,000.00) but not exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both.

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 (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

SEC. 9. Corporate Liability. – When any of the punishable acts herein defined are knowingly 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 in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00).

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 7 up to a maximum of Five million pesos (PhP5,000,000.00).

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

ENFORCEMENT AND IMPLEMENTATION

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 of this Act.

SEC. 11. *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.

SEC. 12. *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.

SEC. 13. *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.

SEC. 14. *Disclosure of Computer Data.* — Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic 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 and the disclosure is necessary and relevant for the purpose of investigation.

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) 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.

SEC. 16. *Custody of Computer Data.* - All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or their contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

SEC. 17. *Destruction of Computer Data.* - Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of a preservation and examination.

SEC. 18. *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.

SEC. 19. *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.

SEC. 20. *Noncompliance.* – Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of *prision correccional* in its maximum period or a fine of One hundred thousand pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.

CHAPTER V

JURISDICTION

SEC. 21. *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

SEC. 22. *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.

CHAPTER VII

COMPETENT AUTHORITIES

SEC. 23. *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 assistance and extradition.

SEC. 24. *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.

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.

SEC. 26. *Powers and Functions.* – The CICC 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 handled 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.

CHAPTER VIII

FINAL PROVISIONS

SEC. 27. *Appropriations.* — The amount of Fifty million pesos (PhP50,000,000.00) shall be appropriated annually for the implementation of this Act.

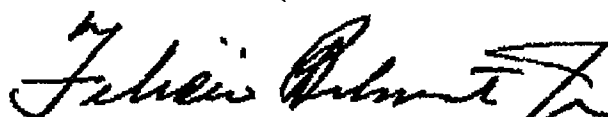
SEC. 28. *Implementing Rules and Regulations.* — The ICTO-DOST, the DOJ and the Department of the Interior and Local Government (DILG) shall jointly formulate the necessary rules and regulations within ninety (90) days from approval of this Act, for its effective implementation.

SEC. 29. *Separability Clause.* — If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 30. *Repealing Clause.* — All laws, decrees or rules inconsistent with this Act are hereby repealed or modified accordingly. Section 33(a) of Republic Act No. 8792 or the "Electronic Commerce Act" is hereby modified accordingly.

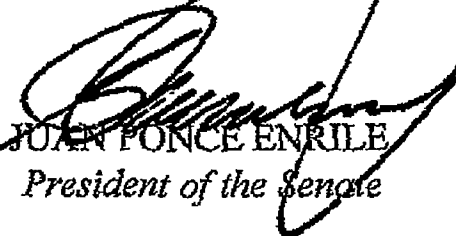
SEC. 31. *Effectivity.* - This Act shall take effect fifteen (15) days after the completion of its publication in the *Official Gazette* or in at least two (2) newspapers of general circulation.

Approved,



FELICIANO BELMONTE JR.

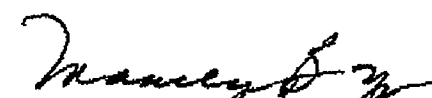
*Speaker of the House
of Representatives*



JUAN PONCE ENRILE

President of the Senate

This Act which is a consolidation of Senate Bill No. 2796 and House Bill No. 5808 was finally passed by the Senate and the House of Representatives on June 5, 2012 and June 4, 2012, respectively.



MARILYN B. BARUA YAP

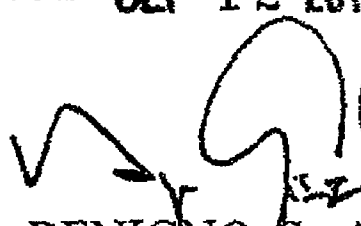
*Secretary General
House of Representatives*



EMMA LIRIO-REYES

Secretary of the Senate

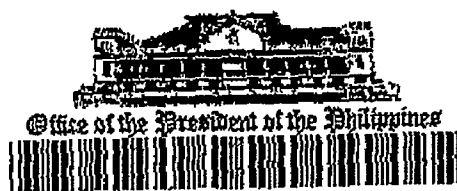
Approved: SEP 12 2012




BENIGNO S. AQUINO III

President of the Philippines

0



PNOY006252