CYBERSECURITY BILL, 2011

CYBERSECURITY BILL, 2011

ARRANGEMENT OF SECTIONS

Sections

A BILL

FOR

AN ACT TO PROVIDE MEASURES FOR NATIONAL CYBERSECURITY AND FOR THE PREVENTION, DETECTION, RESPONSE AND PROSECUTION OF CYBERCRIMES AND OTHER RELATED MATTERS

[ ] Commencement

ENACTED by the National Assembly of the Federal Republic of Nigeria as follows -

PART I - GENERAL PROVISIONS

1 Objects and scope

(1) The objects and scope of this Act are to –

(a) provide an effective legal framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; and

(b) enhance cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs in Nigeria

(2) The provisions of this Act shall be enforced by law enforcement agencies in Nigeria to the extent of the agency's statutory powers.

PART II — OFFENCES AND PENALTIES

2. Unlawful access to a computer

(1) Any Person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network, commits an offence and liable on conviction to imprisonment for a term of 2 years or to a fine of not less than N5,000,000.00 or to both imprisonment and fine.

(2) Where the offence provided in subsection (1) is committed with the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or confidential information, the punishment shall be imprisonment for a term of 3 years or a fine of not less than N7,000,000.00 or to both imprisonment and fine.

(3) Any person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification with the act o omission, commits an offence and liable on conviction to imprisonment for a term of 3 years or to a fine of not less than N7,000,000.00 or to both imprisonment and fine.

3. Unlawful interception of communications

Any person, who intentionally and without authorization, intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting such, to or from a computer, computer system or connected system or network; commits an offence and

liable on conviction to imprisonment for a term of 2 years or to a fine of not less than N5,000,000.00 or to both imprisonment and fine.

4. Unauthorized modification of computer program or data

(1) Any person who directly or indirectly does an act without authority and with intent to cause an unauthorized modification of any program or data held in any computer system or network, commits an offence and liable on conviction to imprisonment for a term of 3 years or to a fine of not less than N7,000,000.00 or to both imprisonment and fine.

(2) Any person who engages in damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority or in excess of authority, commits an offence and liable on conviction to imprisonment for a term of 3 years or to a fine of not less than N7,000,000.00 or to both imprisonment and fine.

(3) For the purpose of this section, a modification of any program or data held in any computer system or network takes place if, by the operation of any function of the computer, computer system or network concerned -

(i) any program or data held in it is altered or erased;

(ii) any program or data is added to or removed from any program or data held in it; or

(iii) any act occurs which impairs the normal operation of any computer, computer system or network concerned.

5. System interference

Any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference in the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and liable on conviction to imprisonment for a term of 2 years or to a fine of not less than N5,000,000.00 or to both imprisonment and fine.

6. Misuse of devices

(1) Any person who unlawfully produces, adapts, manipulates or procures for use, imports , exports, distributes, offers for sale or otherwise makes available -

(a) any devices, including a computer program or a component designed or adapted for the purpose of committing an offence under sections 2, 3, 4 or 5 of this Act;

(b) a computer password, access code or similar data by which the whole or any part of a computer, computer system or network is capable of being accessed for the purpose of committing an offence under this Act, or

(c) any device designed primarily to overcome security measures in any computer, computer system or network with the intent that the devices be utilized for the purpose of violating any provision of this Act,

commits an offence and liable on conviction to imprisonment for a term of 3 years or a fine of not less than N7,000,000.00 or to both imprisonment and fine.

(2) Any person who with intent to commit an offence under this Act, has in his possession any devise or program referred to in subsection 1 of this section, commits an offence and shall be liable on conviction to imprisonment for a term of 2 years or to a fine of not less than N5,000,000.00 or to both imprisonment and fine.

(3) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer or network for any unlawful purpose or gain, commits an offence and shall be liable on conviction to imprisonment for a term of 2 years or to a fine of not less than N5,000,000.00 or to both imprisonment and fine.

(4) Where the offence under subsection (1) of this section results in substantial loss or damage, the offender shall be liable to imprisonment for a term of 5 years or to a fine of not less than N10,000,000.00 or to both imprisonment and fine.

(5) Any person who with intent to commit any offence under this Act uses any automated means or device or any computer program or software to retrieve, collect and store password, access code or any means of gaining access to any program, data or database held in any computer, commits an offence and shall be liable on conviction to imprisonment for a term of 5 years or to a fine of not less than N10,000,000.00 or to both imprisonment and fine.

7. Computer related forgery

Any person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data be considered or acted upon as if it were authentic or genuine, whether or not such data is readable or intelligible, commits an offence and shall be liable on conviction to imprisonment for a term of 3 years or to a fine of not less than N7,000,000.00 or to both imprisonment and fine.

8. Computer related fraud

(1) Any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits whether for himself or another person, commits an offence and shall be liable on conviction to imprisonment for a term of 3 years or to a fine of not less than N7,000,000.00 or to both imprisonment and fine.

(2) Any person who with intent to defraud sends electronic message to a recipient, where such electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of 5 years or to a fine of not less than N10,000,000.00 or to both imprisonment and fine.

9. Child pornography and related offences

(1) Any person who intentionally uses any computer or network system in or for-

(a) producing child pornography for the purpose of its distribution;
(b) offering or making available child pornography;
(c) distributing or transmitting child pornography;
(d) procuring child pornography for oneself or for another person;
(e) possessing child pornography in a computer system or on a computer-data storage medium,

commits an offence under this Act and shall be liable on conviction –

(i) in the case of paragraphs (a), (b) and (c) to imprisonment for a term of 10 years or a fine of not less than N20,000,000.00 or to both imprisonment and fine, and

(ii) in the case of paragraphs (d) and (e) of this subsection, to imprisonment for a term of not less than 5 years or a fine of not less than N10,000,000.00 or to both imprisonment and fine.

(2) For the purpose of subsection (1) above, the term "child pornography" shall include pornographic material that visually depicts:
(a) a minor engaged in sexually explicit conduct;
(b) a person appearing to be a minor engaged in sexually explicit conduct; and
(c) realistic images representing a minor engaged in sexually explicit conduct.

(3) For the purpose of this section, the term "child" or "minor" shall include a person below 16 years of age.

10 Identity theft and impersonation

Any person who in the course of using a computer, computer system or network-

(a) knowingly obtains or possesses another person or entity's identity information with the intent to deceive or defraud, or

(b) fraudulently impersonates another entity or person, living or dead, with intent to -
(i) gain advantage for himself or another person;
(ii) obtain any property or an interest in any property;
(iii) cause disadvantage to the entity or person being impersonated or another person; or
(iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice,

commits an offence and liable on conviction to imprisonment for a term of 3 years or a fine of not less than N7,000,000.00 or to both imprisonment and fine.

11 Cybersquatting

(1) Any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and shall be liable on conviction to imprisonment for a term of 2 years or a fine of not less than N5,000,000.00 or to both imprisonment and fine.

(2) In awarding any penalty against an offender under this section, a court shall have regard to the following -

(a) a refusal by the offender to relinquish, upon formal request by the rightful owner of the name, business name, trademark, domain name, or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria; or

(b) an attempt by the offender to obtain compensation in any form for the release to the rightful owner for use in the Internet of the name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Government of Nigeria.

(3) In addition to the penalty specified under this section, the court may make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.

12 Cyberterrorism

(1) Any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism, commits an offence and liable on conviction to imprisonment for a term of 20 years or to a fine of not less than N25,000,000.00 or to both imprisonment and fine.

(2) For the purposes of this section, terrorism shall have the same meaning under subsection (2) of section 1 of the Terrorism (Prevention) Act, 2011.

13 Racist and xenophobic offences

(1) Any person who -

(a) distributes or otherwise makes available, racist and xenophobic material to the public through a computer system or network,

(b) threatens, through a computer system or network, with the commission of a criminal offence -
(i) persons for the reason that they belong to a group, distinguished by race, colour, descent, national or ethnic origin, as well as, religion, if used as a pretext for any of these factors, or
(ii) a group of persons which is distinguished by any of these characteristics,

(c) insults publicly, through a computer system or network -
(i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or
(ii) a group of persons which is distinguished by any of these characteristics; or

(d) distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or

crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998;

commits an offence and shall be liable on conviction to imprisonment for a term of 5 years or to a fine of not less than N10,000,000.00 or to both imprisonment and fine

(2) For the purpose of subsection (1) above, the term **"**racist and xenophobic material" means any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

14 Records retention and protection of data by service providers

(1) A service provider shall keep all traffic data and subscriber information as may be prescribed by the agency for the time being responsible for the regulation of communication services in Nigeria.

(2) A service provider shall, at the request of the agency referred to in subsection (1) of this section or any law enforcement agency -
   (a) preserve, hold or retain any traffic data, subscriber information or related content, or
   (b) release any information required to be kept under subsection (1) of this section

(3) A law enforcement agency may, through its authorised officer, request for the release of any information in respect of subsection (2) (b) of this section and it shall be the duty of the service provider to comply;

(4) Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction.

(5) Anyone exercising any function under this section shall have due regard to the individual right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.

(6) Any person who contravenes the provisions of subsections (1) – (4) of this section commits an offence and shall be liable on conviction to imprisonment for a term of 3 year or a fine of not less than N7,000,000.00 or to both imprisonment and fine.

15 Interception of electronic communications

Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a Judge may on the basis of information on oath;

(a) order a service provider, through the application of technical means to collect, record, permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorize a law enforcement officer to collect or record such data through application of technical means.

16 Failure of service provider to perform certain duties.

(1) It shall be the duty of every service provider in Nigeria to comply with all the provisions of this Act and disclose any information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding under this Act.

(2) Without prejudice to the generality of the foregoing, a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards -

(a) the identification, apprehension and prosecution of offenders; or

(b) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence; or

(c) the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence or hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.

(3) Any service provider who contravenes the provisions of subsection (1) and (2) of this section, commits an offence and shall be liable on conviction to a fine of not less than N10,000,000.00

(4) In addition to the punishment prescribed under subsection (3) and subject to the provisions of section 18 of this Act, each director, manager or officer of the service provider shall be liable on conviction to imprisonment for a term of 3 years or a fine of not less than N7,000,000.00 or to both such imprisonment and fine.

17 Attempt, conspiracy, aiding and abetting

Any person who -

(a) attempts to commit any offence under this Act; or

(b) does any act preparatory to or in furtherance of the commission of an offence under this Act; or

(c) abets, aids or conspires to commit any offence under this Act,

commits an offence and shall be liable on conviction to the punishment provided for such an offence under this Act.

18 Corporate liability

A body corporate that commits an offence under this Act shall be liable on conviction to a fine of not less than N10,000,000.00 and any person who at the time of the commission of the offence was a chief executive officer, director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable on conviction to

imprisonment for a term of 2 years or a fine of not less than N5,000,000.00 or to both imprisonment and fine;

Provided that, nothing contained in this section shall render any person liable to any punishment if he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of such offence.

PART III – PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

19 Designation of certain computer systems or networks as national critical information infrastructure.

(1) The President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social well being of its citizens, as constituting critical information infrastructure.

(2) The Presidential Order in subsection (1) of this section may prescribe minimum standards, guidelines, rules or procedures in respect of-

(a) the protection or preservation of critical information infrastructure;
(b) the general management of critical information infrastructure;
(c) access to, transfer and control of data in any critical information infrastructure;
(d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical information infrastructure;
(e) the storage or archiving of data or information regarding critical information infrastructure;
(f) disaster recovery plans in the event of loss of the critical information infrastructure or any part thereof; and
(g) any other matter required for the adequate protection, management and control of data and other resources in any critical information infrastructure

20 Audit and Inspection of critical information infrastructure

The Presidential Order under section 19 of this Act, may require audit and inspection to be carried out on any critical information infrastructure, from time to time, to evaluate compliance with the provisions of this Act.

21 Offences against critical information infrastructure

(1) Any person who commits any offence punishable under this Act against any critical information infrastructure designated under section 19 of this Act, shall be liable on conviction to imprisonment for a term of 25 years or a fine of not less than N25,000,000.00 or to both imprisonment and fine.

(2) Where the offence committed under subsection (1) of this section results in serious bodily injury, the offender shall be liable on conviction to imprisonment for a term of not less than 30 years or a fine of not less than N50,000,000.00 or to both imprisonment and fine.

(3) Where the offence committed under subsection (1) of this section results in death, the offender shall be liable on conviction to imprisonment for life.

PART IV – SEARCH, ARREST AND PROSECUTIONS

22 Jurisdiction to try offences under this Act

(1) The Federal High Court or High Court of a State or the Federal Capital Territory shall have jurisdiction to try offences, hear and determine proceedings arising under this Act.

(2) For the purpose of this Act, a person shall be subject to prosecution in Nigeria if the -

(a) offence is committed either wholly or partly within the terror of Nigeria;

(b) act of the offender committed wholly outside Nigeria constitutes a conspiracy to commit an offence under this Act within Nigeria; and an act in furtherance of the conspiracy was committed within Nigeria, either directly by the offender or at his instigation; or

(c) act of the offender committed wholly or partly within Nigeria constitutes an attempt, solicitation or conspiracy to commit an offence in another jurisdiction under the laws of both Nigeria and such other jurisdiction.

(3) For the purpose of this section, an offence is presumed to have been committed in Nigeria if the offence or any of its elements substantially affects a person or interest in Nigeria.

.23 Powers of search and arrest

(1) An authorised officer of any law enforcement agency, entitled to enforce any provision of this Act shall have the power to enter and search any premises or computer or network and arrest any person in connection with any offence committed under this Act.

(2) An authorised officer of any law enforcement agency, upon a reasonable suspicion that an offence has been committed or is about to be committed by any person shall have power at anytime to –

(a) access and inspect or check the operation of any computer, computer system or network to which this Act applies;

(b) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network;

(c) use any technology to re-transform or decrypt any encrypted data contained in a computer into readable text or comprehensible format;

(d) seize or take possession of any computer system used in connection with an offence under this Act;

(e) require any person having charge of or otherwise concerned with the operation of any computer in connection with an offence under this Act to produce such computer;

(f) require any person in possession of encrypted data to provide access to any information necessary to decrypt such data;

(g) require any person in authority to release any subscriber or traffic information or any related content; or

(h) relate with any international law enforcement agencies for the purpose of giving or receiving any information or exchanging any data or database;

for the purposes of investigation and prosecution under this Act.

24 Obstruction

Any person who –

(a) willfully obstructs any law enforcement officer in the exercise of any power under this Act; or

(b) fails to comply with any lawful inquiry or requests made by an authorised officer of any law enforcement agency in accordance with the provisions of this Act,

commits an offence and shall be liable on conviction to imprisonment for a term of 2 years or to a fine of not less than N5,000,000.00 or to both imprisonment and fine.

25 Prosecution of offences

(1) Criminal proceedings under this Act shall be instituted by, with the authority or consent of the Attorney-General of the Federation.

(2) The Attorney - General of the Federation may make rules or regulations with respect to the exercise of his powers under this Act

26 Order of forfeiture of assets

(1) The Court in imposing sentence on any person who is convicted of an offence under this Act, may also order that the convicted person forfeits to the Government of the Federal Republic of Nigeria -

(a) any asset, money or property, whether real or personal, constituting or traceable to gross proceeds of such offence; and

(b) any computer, equipment, software or other technology used or intended to be used to commit or to facilitate the commission of such offence.

(2) Any person convicted of an offence under this Act shall surrender his passport or international travel documents to the Government of the Federal Republic of Nigeria until he has served the sentence or paid the fines imposed on him.

(3) Notwithstanding subsection (2) of this section, the President may -

(a) upon the grant of pardon to the convicted person; or

(b) for the purposes of allowing the convicted person to travel abroad for treatment; or

(c) in the interest of the public;

direct the passport or travel documents of the convicted person be released to him.

27 Order for payment of compensation or restitution

Without prejudice to section 26 of this Act, the Court in imposing sentence on any person convicted under this Act may make an order requiring the convicted person to pay, in addition to any penalty imposed under this Act, monetary compensation to any person or entity for any damage, injury or loss caused to his computer, computer system or network, program or data or to recover any money lost or expended by such person or entity as a result of the offence.

28 Compounding of offences

Without prejudice to section 174 of the Constitution of the Federal Republic of Nigeria, 1999, the Attorney – General of the Federation may, subject to voluntary admission of the commission of the offence, compound any offence punishable under this Act.

PART V – INTERNATIONAL CO-OPERATION

29 Extradition

Offences under this Act shall be extraditable offences under the Extradition Act, CAP E25, Laws of the Federation of Nigeria, 2004.

30 Request for mutual assistance

(1) The Attorney - General of the Federation or designated competent authority may request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act; and may authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act.

(2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreements exist between Nigeria and the requested or requesting country.

(3) The Attorney-General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation if such information will assist in the apprehension of an offender or investigation of any offence under this Act.

31 Evidence pursuant to a request

(1) Any evidence gathered, pursuant to a request under this Act, in any proceedings in the court of any foreign State may, if authenticated, be *prima facie* admissible in any proceedings to which this Act applies.

(2) For the purpose of subsection (1) of this section a document is authenticated if it is -
(a) certified by a Judge or Magistrate of the foreign State; and
(b) sealed by the oath or affirmation of a witness or sealed with an official or public seal -

(i) of a Ministry or Department of the Government of the foreign State; or
(ii) in the case of a territory, protectorate or colony, of the person administering the Government of the foreign territory, protectorate or colony or a department of that territory, protectorate or colony.

32 Form of request

(1) A request under this part of this Act shall be in writing, dated and signed by or on behalf of the person making the request.

(2) A request may be transmitted by facsimile or by any other electronic device or means; and shall -

(a) confirm either that an investigation or prosecution is being conducted in respect of a suspected offence related to computer crimes and cybersecurity or that a person has been convicted of an offence related to cybercrimes and cybersecurity;

(b) state the grounds on which any person is being investigated or prosecuted for an offence related to computer crimes and cybersecurity or details of the conviction of the person;

(c) give sufficient particulars of the identity of the person;

(d) give sufficient particulars to identify any financial institution or designated non - financial institution or other persons believed to have information, documents or materials which may be of assistance to the investigation or prosecution;

(e) specify the manner in which and to whom any information, document or material obtained pursuant to the request is to be produced;

(f) state whether-
(i) a forfeiture Order is required, or
(ii) the property may be made the subject of such an Order; and

(g) contain such other information as may assist in the execution of the request.

(3) A request shall not be invalidated for the purposes of this Act or any legal proceedings by failure to comply with the provision of subsection (2) of this section where the Attorney-General of the Federation is satisfied that there is sufficient compliance to enable him execute the request.

(4) Where the Minister charged with responsibility for finance considers it appropriate, either because an international arrangement so requires or permits or it is in the public interest, he shall after obtaining the approval of the Government order that the whole or any part of any property forfeited under this Act or the value thereof, be returned or remitted to the requesting State.

33 Preservation and expedited disclosure of computer data within international cooperation

(1) Nigeria may be requested to expedite preservation of data stored in a computer system located in Nigeria, referring to crimes described under this Act, pursuant to the submission of a request for assistance for search, seizure and disclosure of those data.

(2) The request under subsection (1) of this section shall specify:
a) the authority requesting the preservation or disclosure;
b) the offence being investigated or prosecuted, as well as a brief statement of the facts relating thereto;
c) the computer data to be retained and its relation to the offence;
d) all the available information to identify the person responsible for the data or the location of the computer system;
e) the necessity of the measure of preservation, and
f) the intention to submit a request for assistance for search, seizure and disclosure of the data.

(3) In executing the demand of a foreign authority under the preceding sections, the Attorney - General of the Federation may order any person who has the control or availability of such data, including a service provider, to preserve them.

(4) Without prejudice to the provisions of subsection (3) of this section, the preservation may also be ordered by any law enforcement agency, with the responsibility for enforcing any provisions of this Act, pursuant to an order of court, which order may be obtained ex parte where there is urgency or danger in delay.

(5) Where a court grants an order, pursuant to the provisions of subsection (4) of this section, such order shall indicate:

(a) the nature of data;
(b) their origin and destination, if known; and
(c) the period of time over which data must be preserved.

(6) In compliance with the preservation order, any person who has the control or availability of such data, including a service provider, shall immediately preserve the data for the specified period of time, protecting and maintaining its integrity.

(7) A request for expedited preservation of computer data may be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be denied for lack of verification of dual criminality.

34 Designation of contact point for 24/7 Network

(1) In order to provide immediate assistance for the purpose of international cooperation under this Act, the National Security Adviser shall designate and maintain a contact point that shall be available twenty-four hours a day, seven days a week.

(2) This contact point can be contacted by other contact points in accordance with agreements, treaties or conventions to which Nigeria is bound, or in pursuance of protocols of cooperation with international judicial or law enforcement agencies.

(3) The immediate assistance to be provided by the contact point shall include:

a) technical advice to other points of contact;

b) expeditious preservation of data in cases of urgency or danger in delay;

c) collection of evidence for which it has the legal jurisdiction in cases of urgency or danger in delay;

d) detection of suspects and providing of legal information in cases of urgency or danger in delay;

e) the immediate transmission of requests concerning the measures referred to in paragraghs (b) and (d) of subsection (3) of this section, with a view to its expedited implementation.

PART VI – MISCELLANEOUS

35 Directives of a general character

The President may issue to any agency responsible for implementing or enforcing any provisions of this Act, any directive of a general character or relating to particular matter with regard to the exercise by that agency of its functions and it shall be the duty of that agency to comply with the directive.

36 Regulations

(1) The National Security Adviser may make such regulations as may be necessary for the effective enforcement of this Act.

(2) The contravention of any regulation issued pursuant to subsection (1) of this section shall constitute an offence and shall be punishable as prescribed in the particular regulation.

37 Interpretation.

In this Act, unless the context otherwise requires -

Access - in relation to an application or data, means rendering that application or data, by whatever means, in a form that would enable a person, at the time when it is so rendered or subsequently, to take account of that application or data including using the application or data or having its output from the computer system in which it is held in a displayed or printed Form, or to a storage medium or by means of any other output device, whether attached to the computer system in which the application or data are held or not;

application" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function, and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system

Authorized Access - A person has authorized access to any program or data held in a computer if—

(a) the person is entitled to control access to the program or data in question; or

(b) the person has consent to access such program or data from a person who is charged with giving such consent.

Authorized Officer or Authorized persons - means duly authorized officers of any law enforcement officers involved in the prevention, elimination or combating of computer crimes and cyber security threats

Computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

Computer Data - Computer data is information required by the computer to be able to operate. It is used to run programs, store programs and store information that the computer user needs such as text files or other files that are associated with the program the computer user is running.

Computer Network - means a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information. Networks may be classified according to a wide variety of characteristics such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope. The rules and data formats for exchanging information in a computer network are defined by communications protocols.

Computer Program - A computer program (also software, or just a program) is a sequence of instructions written to perform a specified task with a computer. A computer requires programs to function, typically executing the program's instructions in a central processor. The program has an executable form that the computer can use directly to execute the instructions. The same program in its human-readable source code form, from which executable programs are derived (e.g., compiled), enables a programmer to study and develop its algorithms.

Content Data - means information stored on a computer system memory

Critical Infrastructure - Critical infrastructure includes assets, systems and networks, whether physical or virtual, so vital to the security , defence or international relations of Nigeria; the provisions of service directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure or the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services

Damage - means any impairment to a computer or the integrity or availability of data, program, system or information that—

(i) causes loss aggregating at least One Million Naira in value, or such other amount as the National Security Adviser may, by notification in the Gazette prescribe, except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken in to account;

(ii) modifies or impairs, or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(iii) causes or threatens physical injury or death to any person; or

(iv) threatens public health or public safety

Data - means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer

Database - Digitally organized collection of data for one or more purposes. It allows easy access, management and update of data

Device - Any object whose mechanical and/or electrical workings are controlled or monitored by a microprocessor

Electronic communication – includes **c**ommunications in electronic format, instant messages, short message service (sms), e-mail, video, voice mails, multimedia message service (MMS), Fax, and pager.

Electronic Record - means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another

Function - includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer

Interception - in relation to a function of a computer system or communications network, includes listening to or recording of communication data of a computer or acquiring the substance, meaning or purport of such and any acts capable of blocking or preventing any of these functions.

Law Enforcement Agencies - includes any agency for the time being responsible for implementation and enforcement of the provisions of this Act.

Malware -consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code

Network – means a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information.

Person – includes an individual, body corporate, organisation or group of persons

President - means the President and Commander in – Chief of the Armed Forces of the Federal Republic of Nigeria

Service provider means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

Traffic Data --- means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

38 Short Title

This Act may be cited as the Cybersecurity Act, 2011

EXPLANATORY MEMORANDUM

(This note does not form part of the above Act but is intended to explain its purport)

The Bill seeks to provide measures for national cybersecurity and for the prevention, detection, response and prosecution of cybercrimes and other related matters.