# CYBERCRIME ACT 2015

## CYBERCRIME BILL, 2015

ARRANGEMENT OF SECTIONS

**Section**

**A BILL FOR AN ACT TO PROVIDE FOR THE PROHIBITION, PREVENTION, DETECTION, RESPONSE AND PROSECUTION OF CYBERCRIMES AND FOR OTHER RELATED MATTERS, 2013**

[ ] Commencement

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

## PART I OBJECT AND APPLICATION 1. Objectives

The objectives of this Act are to –

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

(b) ensure the protection of critical national information infrastructure; and

(c) promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.

## 2. Application

The provisions of this Act shall apply throughout the Federal Republic of Nigeria

## PART II PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

## 3. Designation of certain computer systems or networks as critical national 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 National Information Infrastructure.

(2) The Presidential Order made under subsection (1) of this section may prescribe minimum standards, guidelines, rules or procedure 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 national information infrastructure;

(e) the storage or archiving of data or information regarded critical national information infrastructure;

(f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and

(g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure

## 4. Audit and Inspection of critical national information infrastructure

The Presidential Order made under section 3 of this Act may require the audit and inspection of any Critical National Information Infrastructure, from time to time, to evaluate compliance with the provisions of this Act.

## PART III OFFENCES AND PENALTIES

### 5. Offences against critical national information infrastructure

(1) Any person who commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to section 3 of this Act, is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine.

(2) Where the offence committed under subsection (1) of this section results in grievous bodily injury, the offender shall be liable on conviction to imprisonment for a minimum term of 15 years without option of fine.

(3) Where the offence committed under subsection (1) of this section results in death, the offender shall be liable on conviction to death sentence without out option of fine.

### 6. 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 not less than two years or to a fine of not less than ₦5,000,000 or to both fine and imprisonment.

(2) Where the offence provided in subsection (1) of this section 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 not less than three years or a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

(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 or omission, commits an offence and liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

### 7. Unlawful interception of communications

Any person, who intentionally and without authorization or in excess of authority, 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 signals, 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 not less than two years or to a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

**8. Unauthorized modification of computer data**

(1) Any person who directly or indirectly does an act without authority and with intent to cause an unauthorized modification of any data held in any computer system or network, commits an offence and liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

(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 not less than three years or to a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

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

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

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

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

**9. 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 not less than two years or to a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

**10. Misuse of devices**

(1) Any person who unlawfully produces, supplies, 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 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 is liable on conviction to imprisonment for a term of not less than three years or a fine of not less than ₦7,000,000.00 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 not less than two years or to a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

(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 not less than two years or to a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

(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 not less than five years or to a fine of not less than ₦10,000,000.00 or to both fine and imprisonment.

(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 not less than five years or to a fine of not less than ₦10,000,000.00 or to both fine and imprisonment.

## 11. 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 will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

## 12. 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 for himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or to a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

(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 not less than five years or to a fine of not less than ₦10,000,000.00 or to both fine and imprisonment.

## 13. 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's 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 not less than three years or a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

## 14. 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 is liable on conviction –

(i) in the case of paragraphs (a), (b) and (c) to imprisonment for a term of ten years or a fine of not less than ₦20,000,000.00 or to both fine and imprisonment, and

(ii) in the case of paragraphs (d) and (e) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than ₦10,000,000.00 or to both fine and imprisonment.

(2) Any person who, intentionally proposes, grooms or solicits, through information and communication technologies, to meet a child, followed by material acts leading to such a meeting for the purpose of:

(a) engaging in sexual activities with a child;

(b) engaging in sexual activities with a child where -

(i) use is made of coercion, inducement, force or threats;

(ii) abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or

(iii) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence;

(c) recruiting, inducing, coercing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes;

commits an offence under this Act and is liable on conviction-

(i) in the case of paragraphs (a) and (b) to imprisonment for a term of not less than 10 years or a fine of not less than ₦15,000,000 or to both fine and imprisonment; and

(ii) in the case of paragraph (c) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than ₦10,000,000 or to both fine and imprisonment.

(3) 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.

(4) For the purpose of this section, the term “child” or “minor” shall include a person below 18 years of age.

**15. Cyberstalking**

(1) Any person who, by means of a public electronic communications network persistently sends a message or other matter that -

(a) is grossly offensive or of an indecent, obscene or menacing character or causes any such message or matter to be so sent; or

(b) he knows to be false, for the purpose of causing annoyance, inconvenience or needless anxiety to another or causes such a message to be sent;

commits an offence under this Act and shall be liable on conviction to a fine of not less than ₦2,000,000.00 or imprisonment for a term of not less than one year or to both fine and imprisonment.

(2) Any person who, through information and communication technologies, by means of a public electronic communications network, transmits or causes the transmission of any communication –

(a) with intent to bully, threaten or harass another person, where such communication places another person in fear of death, violence or personal bodily injury or to another person;

(b) containing any threat to kidnap any person or any threat to injure the person of another, any demand or request for a ransom for the release of any kidnapped person, with intent to extort from any person, firm, association or corporation, any money or other thing of value; or

(c) containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, with intent to extort from any person, firm, association, or corporation, any money or other thing of value;

commits an offence under this Act and is liable on conviction-

(i) in the case of paragraphs (a) and (b) of this subsection to imprisonment for a term of not less than ten years or a fine of not less than ₦25,000,000 or to both fine and imprisonment; and

(ii) in the case of paragraph (c) of this subsection, to imprisonment for a term of not less than five years or a fine of not less than ₦15,000,000.00 or to both fine and imprisonment.

(3) A court sentencing or otherwise dealing with a person convicted of an offence under subsections (1) and (2) may (as well as sentencing him or dealing with him in any other way) make an order, which may, for the purpose of protecting the victim or victims of the offence, or any other person mentioned in the order, from further conduct which- (a) amounts to harassment, or

(b) will cause a fear of violence, death or bodily injury; prohibit the defendant from doing anything described/specified in the order.

(4) A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence under this section and shall be liable on conviction to a fine of not less than ₦10,000,000.00 or imprisonment for a term of not less than three years or to both fine and imprisonment.

(5) The order made under subsection (3) of this section may have effect for a specified period or until further order and the defendant or any other person mentioned in the order may apply to the court which made the order for it to be varied or discharged by a further order.

## 16. 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 is liable on conviction to imprisonment for a term of not less than two years or a fine of not less than ₦5,000,000.00 or to both fine and imprisonment.

(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.

**17. 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 life imprisonment.

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

**18. Racist and xenophobic offences**

(1) Any person who -

(a) distributes or otherwise makes available, any 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 not less than five years or to a fine of not less than ₦10,000,000.00 or to both fine and imprisonment.

(2) For the purpose of subsection (1) of this section, 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.

**19. 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 is liable on conviction to the punishment provided for the principal offence under this Act.

**20. Corporate liability**

(1) A body corporate that commits an offence under this Act shall be liable on conviction to a fine of not less than ₦10,000,000.00 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 not less than two years or a fine of not less than ₦5,000,000.00 or to both fine and imprisonment;

(2) Nothing contained in this section shall render any person liable to any punishment where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.

## PART IV DUTIES OF SERVICE PROVIDERS

### 21. Records retention and protection of data

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

(2) A service provider shall, at the request of the relevant authority 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's 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) Subject to the provisions of section 20 of this Act, any person or entity who contravenes any of the provisions of this section commits an offence and is liable on conviction to imprisonment for a term of not less than three year or a fine of not less than ₦7,000,000.00 or to both fine and imprisonment .

### 22. 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.

**23. 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;

(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 ₦10,000,000.00.

(4) In addition to the punishment prescribed under subsection (3) of this section and subject to the provisions of section 20 of this Act, each director, manager or officer of the service provider shall be liable on conviction to imprisonment for a term of not less than three years or a fine of not less than ₦7,000,000.00 or to both fine and imprisonment.

## PART V ADMINISTRATION AND ENFORCEMENT

### 24. Co-ordination and enforcement

(1) The Office of the National Security Adviser shall be the co-coordinating body for all security and enforcement agencies under this Act and shall;

(a) provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria;

(b) ensure the effective formulation and implementation of a comprehensive cybersecurity strategy for Nigeria;

(d) build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under this Act or any other law on cybercrime in Nigeria; and

(e) do such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act.

(2) The Attorney – General of the Federation (in this Act referred to as "Minister") shall be the coMinister for the effective implementation and administration of this Act; and shall strengthen and enhance the existing legal framework to ensure -

(a) conformity of Nigeria's cybercrime and cybersecurity laws and policies with international standards and the African Union Conventions on Cybersecurity;

(b) maintain international co-operation required for preventing and combating cybercrimes and promoting cybersecurity; and

(c) effective prosecution of cybercrimes and cybersecurity matters.

(3) All law enforcement, security and intelligence agencies shall develop requisite institutional capacity for the effective implementation of the provisions of this Act and shall in collaboration with the National Security Adviser, initiate, develop or organize training programmes nationally or internationally for officers charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.

### 25. Establishment of the Cybercrime Advisory Council

(1) There is established, a Cybercrime Advisory Council (in this Act referred to as "the Council") which shall comprise of a representative each of the Ministries and Agencies listed under the Schedule to this Act.

(2) A representative appointed pursuant to subsection (1) of this section shall be an officer not below the Directorate Cadre in the Public Service or its equivalent.

(3) The Council shall create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cybersecurity in Nigeria.

(5) A member of the Council shall cease to hold office if –

(a) he ceases to hold the office on the basis of which he became a member of the Council; or

(b) the President is satisfied that it is not in the public interest for the person to continue in office as a member of the Council.

(6) The meetings of the Council shall be presided over by the National Security Adviser.

(7) The Council shall meet at least four times in a year and whenever it is convened by the National Security Adviser.



**26. Functions and powers of the Council**

(1) The Council shall -

(a) formulate and provide general policy guidelines for the implementation of the provisions of this Act; and

(b) advice on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues.

(2) The Council shall have power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as Council may, from time to time determine.

## PART VI SEARCH, ARREST AND PROSECUTION

### 27. Power to conduct search and arrest

(1) A law enforcement officer duly authorized may apply *ex-parte* to the court for the issuance of a warrant for the purposes of a cybercrime or computer related crime investigation.

(2) The court may issue a warrant authorizing a law enforcement officer to- (a) enter the premises or conveyance specified or described in the warrant;

(b) search the premises or conveyance and any person found therein; and

(c) seize and retain any computer or electronic device and relevant material found therein.

(3) The court shall not issue a warrant under subsection (2) of this section unless the court is satisfied
that -

(a) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act; or

(b) for the purpose of investigating cybercrime, cybersecurity breach or computer related offences; or

(c) there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation; and

(d) the person named in the warrant is preparing to commit an offence under this Act.

### 28. Powers to conduct investigation or search without warrant

(1) Where in a case of verifiable urgency, a cybercrime or computer related offences is threatened, or there is the urgent need to prevent the commission of an offence provided under this Act, and an application to the court or to a Judge in Chambers to obtain a warrant would cause delay that
may be prejudicial to the maintenance of public safety or order, an authorized law enforcement officer may without prejudice to the provisions of section 27 of this Act or any other law; with the assistance of such other authorized officers as may be necessary and while search warrant is being sought for -

(a) enter and search any premises or place if he has reason to suspect that, within those premises, place or conveyance -
    (i) an offence under this Act is being committed or likely to be committed; or
    (ii) there is evidence of the commission of an offence under this Act; or
    (iii) there is an urgent need to prevent the commission of an offence under this Act

(b) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (a) of this subsection;

(c) stop, board and search any conveyance where the authorised officer has reasons to suspect that there is evidence of the commission or likelihood of the commission of an offence under this Act;

(d) seize, remove and detain anything which is, or contains or appears to him to be or to contain evidence of the commission of an offence under this Act; or

(e) 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;

(f) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format;

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

(h) arrest, search and detain any person whom the officer reasonably suspects of having committed or likely to commit an offence under this Act.

(2) Where a seizure is effected in the course of search or investigation under this Act, a copy of the list of all the items, documents and other materials seized shall be made, duly endorsed and handed to the-
    (a) person on whom the search is made; or
    (b) owner of the premises, place or conveyance seized.

(3) Notwithstanding the provisions of subsection (1) of this section, a woman shall only be searched by a woman.

(4) Nothing in this section shall be construed as derogating from the lawful right of any person in defence of his person or property.

(5) A duly authorized law enforcement officer who uses such force as may be reasonably necessary
for any purpose in accordance with this Act, shall not be liable in any criminal or civil proceedings, for having, by the use of reasonable force caused injury or death to any person or damage to or loss of any property.

**29. Obstruction and refusal to release information.**

Any person who –

(a) willfully obstructs any authorized law enforcement officer in the exercise of any powers conferred by this Act; or

(b) fails to comply with any lawful inquiry or requests made by an authorized 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 two years or to a fine of not less than ₦500,000.00 only or to both fine and imprisonment.

**30. Prosecution of offences**

The Attorney-General of the Federation shall prosecute offences under this Act subject to the provisions of the Constitution of the Federal Republic of Nigeria, 1999.

**31. Order of forfeiture of assets.**

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

(a) any asset, money or property, whether tangible or intangible, constituting or traceable to proceeds of such offence; and

(b) any computer, equipment, software or electronic device and other technological device used or intended to be used to commit or to facilitate the commission of such offence;

(2) Where it is established that a convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities listed in this Act, such assets or properties, shall subject to any Treaty or arrangement with such foreign country, be forfeited to the Federal Government of Nigeria.

(4) The office of the Attorney-General of the Federation shall ensure that the forfeited assets or properties are effectively transferred and vested in the Federal Government of Nigeria.

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

(4) Notwithstanding subsection (2) of this section, the President may upon the grant of pardon to the convicted person -

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

(b) in the public interest;

direct that the passport or travel documents of the convicted person be released to him on the recommendation of the Minister.

**32. Order for payment of compensation or restitution**

Without prejudice to section 31 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 on him 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 being convicted for.

## PART VII JURISDICTION AND INTERNATIONAL CO-OPERATION

**33. Jurisdiction**

(1) The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed or High Court of Federal Capital Territory shall have jurisdiction to try offences under this Act committed - (a) in Nigeria; or

(b) on a ship or aircraft registered in Nigeria; or

(c) by a Nigerian outside Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or

(d) outside Nigeria, where -

(i) the victim of the offence is a citizen or resident of Nigeria; or

(ii) the alleged offender is in Nigeria and not extradited to any other country for prosecution.

(2) The Federal High Court shall have jurisdiction to impose any penalty provided for an offence under this Act or any other related law.

(3) In the trial of any offence under this Act, the fact that an accused person is in possession of- (a) pecuniary resources or property for which he cannot satisfactorily account for; or

(b) which is disproportional to his known sources of income; or

(c) that he had at or about the time of the alleged offence obtained an accretion to his pecuniary resources or property for which he cannot satisfactorily account for,

may be relevant prove of commission of the alleged offence and shall be taken into account by the court as corroborating the testimony of any other witness in the course of his trial.

(4) In any trial for an offence under this Act, the Court shall have power, notwithstanding anything to the contrary in any other enactment, adopt all legal measures necessary to avoid unnecessary delays and abuse in the conduct of matters.

(5) Subject to the provisions of the Constitution of the Federal Republic of Nigeria, an application for stay of proceedings in respect of any criminal matter brought under this Act shall not be entertained until judgment is delivered.

**34. Extradition**

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

**35. 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.

**36. 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, is *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 or Notary Public of the foreign State; and

(b) sworn to under 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.

**37. Form of request**

(1) A request under 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 Attorney-General of the Federation considers it appropriate because an international arrangement so requires or it is in the public interest, he shall 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.

**38. Expedited Preservation of computer data.**

(1) Nigeria may be requested to expedite the preservation of data stored in a computer system or network, referring to crimes described under this Act or any other enactment, 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 or turn them in for proper preservation by an appropriate authority or person.

(4) Without prejudice to the provisions of subsection (3) of this section, the preservation may also be requested by any law enforcement agency, with 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.

**39. Designation of contact point.**

(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 and 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 paragraphs (b) and (d) of subsection (3) of this section, with a view to its expedited implementation.

## PART VIII MISCELLANEOUS

### 40. 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.

### 41. Regulations

(1) The Minister may make orders, rules, guidelines or regulations as are necessary for the efficient implementation of the provisions of this Act.

(2) Orders, rules, guidelines or regulations made under subsection (1) of this section may provide for the -

(a) method of custody of video and other electronic recordings of suspects apprehended under this Act;

(b) method of compliance with directives issued by relevant international institutions cybersecurity and cybercrimes;

(c) procedure for freezing, unfreezing and providing access to frozen funds or other assets;

(d) procedure for attachments, forfeiture and disposal of assets,

(e) mutual legal assistance,

(f) procedure for the prosecution of all cybercrime cases in line with national and international human rights standards; and

(g) any other matter the Attorney - General may consider necessary or expedient for the purpose of the implementation of this Act.

**42. Interpretations**

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 prohibition, 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"*** include information required by the computer to be able to operate, 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...

***"computer program"*** means a sequence of instructions written to perform a specified task with a computer.

***"content data"*** means information stored on a computer system memory.

***"critical national information 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.

the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include false accusations, monitoring, making threats,

***"cyberstalking"*** includes -

(i) identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass;

(ii) sending multiple e-mails, often on a systematic basis, to annoy, embarrass, intimidate, or threaten a person or to make the person fearful that she or a member of her family or household will be harmed.

***"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"*** means digitally organized collection of data for one or more purposes which allows easy access, management and update of data;

***"device"*** means any object whose mechanical 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 behaviour including but not limited to a variety of forms of hostile, intrusive, or annoying software or program code;

***"Minister"*** means the Attorney – General of the Federation and Honourable Minister of Justice;

***"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;

*"**Sexually explicit conduct**"* includes at least the following real or simulated acts-

(a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex;

(b) bestiality;

(c) masturbation;

(d) sadistic or masochistic abuse in a sexual context; or

(e) lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the conduct depicted is real or simulated; and

***"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.

**43. Short title**

This Act may be cited as the Cybercrime Act, 2013.

# SCHEDULE

**MEMBERS OF THE CYBERCRIME ADVISORY COUNCIL**

(1) The Cybercrime Advisory Committee shall comprise of a representative each of the following Ministries,
Departments and Agencies

(a) Federal Ministry of Justice;
(b) Federal Ministry of Finance;
(c) Ministry of Foreign Affairs
(d) Federal Ministry of Trade and Investment
(e) Central Bank of Nigeria;
(f) National Security Adviser;
(g) State Security Service;
(h) Nigeria Police Force;
(i) Economic and Financial Crimes Commission,
(j) Independent Corrupt Practices Commission;
(k) Nigerian Intelligence Agency;
(l) Nigerian Civil Defence Corps;
(m) Defence Intelligent Agency;
(n) Military Intelligent Agency;
(o) National Agency for the Prohibition of Traffic in Persons;
(p) Nigerian Customs Service;
(q) Nigerian Immigration Service;
(r) Nigerian Financial Intelligence Agency.
(s) National Space Management Agency
(t) Nigerian Information Technology Development Directorate (u) Nigerian Communications Commission

(2) The Cybercrime Advisory Council shall also comprise of a representative of any other Ministry, Department, Agency or Institution which the Minister may by notice published in the Federal Gazette add to the list under paragraph 1 of this Schedule

## EXPLANATORY MEMORANDUM

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

The Act seeks to provide an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; ensure the protection of critical national information infrastructure; and promote cybersecurity and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights.