Proclamation No. ……/2016

A PROCLAMATION TO PROVIDE FOR THE COMPUTER CRIME

WHEREAS information and communication technology plays a vital role in the economic, social and political development of the country;

WHEREAS unless appropriate protection and security measures are taken, the utilization of information communication technology is vulnerable to various computer crimes and other security threats that can impede the overall development of the country and endanger individual rights;

WHEREAS the existing laws are not adequately tuned with the technological changes and are not sufficient to prevent, control, investigate and prosecute the suspects of computer crimes;

WHEREAS it has become necessary to incorporate new legal mechanisms and procedures in order to prevent, control, investigate and prosecute computer crimes and facilitate the collection of electronic evidences;

NOW, THEREFORE, in accordance with Article 55(1) of the Constitution of the Federal Democratic Republic of Ethiopia, it is hereby proclaimed as follows:

PART ONE
GENERAL

1. Short Title

This Proclamation may be cited as the "Computer Crime Proclamation No. ----------/2016".

2. Definitions

In this Proclamation unless the context otherwise requires:

1/ "data processing service" means the service of reception, storage, processing, emission, routing or transmission of data by means of computer system and includes networking services;

2/ "computer or computer system" means any software and the microchips technology based data processing, storage, analysis, dissemination and communication device or any device that is capable of performing logical, arithmetic or routing function and includes accessories of that device;

3/ "computer data" means any content data, traffic data, computer program, or any other subscriber information in a form suitable for processing by means of a computer system;

4/ "computer program" means a set of instructions or commands expressed in words, codes or schemes which are capable of causing a computer system to perform or achieve a particular task or result;

5/ "traffic data" means any computer generated data relating to a chain of communication by means of a computer system indicating the communication's origin, destination, route, time, date, duration, size or types of underlying service;

6/ "content data" means any computer data found in the form of audio, video, picture, arithmetic formula or any other form that conveys the essence, substance, meaning or purpose of a stored or transmitted computer data or computer communication;

7/ "network" means the interconnection of two or more computer systems by which data processing service can be provided or received;

8/ "computer data security" means the protection of a computer data from deleting, changing, and accessing by unauthorized person, compromising its confidentiality or any other damage;

9/ "access" means to communicate with, to enter in, store in, store data in, retrieve, or obtain data from, to view, to receive, move or copy data from a computer system, or otherwise make use of any data processing service thereof;

10/ "critical infrastructure" means a computer system, network or data where any of the crimes stipulated under article 3 to 6 of this proclamation, is committed against it, would have a considerable damage on public safety and the national interest;

11/ "interception" means real-time surveillance, recording, listening, acquisition, viewing, controlling or any other similar act of data processing service or computer data;

12/ "spam" means unsolicited e-mails transmitted to multiple electronic accounts at a time;

13/ "service provider" means a person who provides technical data processing or communication service or alternative infrastructure to users by means of computer system;

14/ "Ministry" or "Minister" means the Ministry or Minister of Justice, respectively;

15/ "Public Prosecution Department" means federal public prosecutor department legally vested with the power and function of prosecution or delegated regional state public prosecutor departments;

16/ "investigatory organ" mean a person legally invested with the power of investigation;

17/ "regional state" means any state referred to in Article 47(1) of the Constitution of the Federal Democratic Republic of Ethiopia and for the purpose this Proclamation it includes Addis Ababa and Dire Dawa city administrations;

18/ "police" mean Federal Police or Regional State Police to whom the power of the Federal Police is delegated;

19/ "Agency" mean Information Network Security Agency;

20/ "person" means a physical or juridical person;

21/ any expression in the masculine gender includes the feminine.

PART TWO
COMPUTER CRIMES
SECTION ONE
CRIMES AGAINST COMPUTER SYSTEM AND COMPUTER DATA

3. Illegal Access

1/ Whosoever, without authorization or in excess of authorization, intentionally secures access to the whole or any part of computer system, computer data or network shall be punishable with simple imprisonment not exceeding three years or fine from Birr 30,000 to 50, 000 or both.

2/ Where the crime stipulated under sub-article (1) of this Article is committed against:

a) a computer system, computer data or network that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three to five years and fine from Birr 30,000 to 50,000;

b) a critical infrastructure, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000.

4. Illegal Interception

1/ Whosoever, without authorization or in excess of authorization, intentionally intercepts non-public computer data or data processing service shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.

2/ Where the crime stipulated under sub-article (1) of this Article is committed against:

a) a computer data or data processing service that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000.

b) a critical infrastructure, the punishment shall be rigorous imprisonment from 10 to 15 years and fine from Birr 100,000 to 200,000.

5. Interference with Computer System

1/ Whosoever, without authorization or in excess of authorization, intentionally hinders, impairs, interrupts or disrupts the proper functioning of the whole or any part of computer system by inputting, transmitting, deleting or altering computer data shall be punishable with rigorous imprisonment from three years to five years and fine not exceeding Birr 50,000.

2/ where the crime stipulated under sub-article (1) of this Article is committed against:

a) a computer system that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000;

b) a critical infrastructure, the punishment shall be rigorous imprisonment from 10 years to 20 years.

6. Causing Damage to Computer Data

1/ Whosoever, without authorization or in excess of authorization, intentionally alters, deletes, suppresses a computer data, renders it meaningless, useless or inaccessible to authorized users shall be punishable with rigorous imprisonment not exceeding three years and fine not exceeding Birr 30,000.

2/ Where the crime stipulated under sub-article (1) of this Article is committed against:

a) a computer data that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three years to five years and fine from Birr 30,000 to 50,000;

b) a critical infrastructure, the punishment shall be rigorous imprisonment from five to 10 years and fine from Birr 50,000 to 100,000.

7. Criminal Acts Related to Usage of Computer Devices and Data

1/ Whosoever, knowing that it can cause damage to computer system, computer data or network, intentionally transmits any computer program exclusively designed or adapted for this purpose shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 50,000.

2/ Whosoever, knowing that it is to be used for the commission of unlawful act specified under Articles 3 to 6 of this Proclamation, intentionally imports, produces, offers for sale, distributes or makes available any computer device or computer program designed or adapted exclusively for the purpose of committing such crimes shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.

3/ Whosoever possesses any computer devices or data specified under sub-article (1) or (2) of this Article with the intention to further the commission of any of the crimes specified under Articles 3 to 6 of this Proclamation shall be punishable with simple imprisonment not exceeding three years or fine from Birr 5,000 to 30, 000.

4/ Whosoever, without authorization or in excess of authorization, intentionally discloses or transfers any computer program, secret code, key, password or any other similar data for gaining access to a computer system, computer data or network shall be punishable with simple imprisonment not exceeding five years or in serious cases with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000.

5/ Where the crime stipulated under sub-article (4) of this Article is committed negligently, the punishment shall be simple imprisonment not exceeding one year and fine.

8. Aggravated Cases

Where the crime stipulated under Article 3 to 6 of this Proclamation is committed against a computer data or a computer system or network which is designated as top secrete by the concerned body for military interest or international relation, and while the country is at a state of emergency or threat, the punishment shall be rigorous imprisonment from 15 to 25 years.

SECTION TWO
COMPUTER RELATED FORGERY, FRAUD AND THEFT

9. Computer Related Forgery

Whosoever falsifies a computer data, makes false computer data or makes use of such data to injure the rights or interests of another or to procure for himself or for another person any undue right or advantage shall be punishable with simple imprisonment not exceeding three years and fine not exceeding Birr 30,000 or in a serious cases with rigorous imprisonment not exceeding 10 years and fine from Birr 10,000 to 100,000.

10. Computer Related Fraud

1/ Whosoever fraudulently causes a person to act in a manner prejudicial to his rights or those of third person by distributing misleading computer data, misrepresenting his status, concealing facts which he had a duty to reveal or taking advantage of the person's erroneous beliefs, shall be punishable with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.

2/ Whosoever, with fraudulent intent of procuring any benefit for himself or for another person, causes economic loss to another person by any change, deletion or any other damage of computer data shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000 or in serious cases with rigorous imprisonment not exceeding 10 years and fine from Birr 10,000 to 100,000.

11. Electronic Identity Theft

Whosoever, with intent to commit criminal act specified under Article 10 of this Proclamation or for any other purpose produces, obtains, sales, possesses or transfers any data identifying electronic identity of another person without authorization of that person shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 50,000.

SECTION THREE
ILLEGAL CONTENT DATA

12. Obscene or Indecent Crimes Committed Against Minors

1/ Whosoever intentionally produces, transmits, sales, distributes, makes available or possesses without authorization any picture, poster, video or image through a computer system that depicts:

a) a minor engaged in sexually explicit conduct; or

b) a person appearing to be a minor engaged in sexually explicit conduct;

shall be punishable with rigorous imprisonment from three years to 10 years.

2/ Whosoever entices or solicits a minor for sexual explicit conduct by transmitting or sending erotic speeches, pictures, text messages or videos through computer system shall be punishable with rigorous imprisonment from five to 10 years.

13. Crimes against Liberty and Reputation of Persons

Whosoever intentionally:

1/ intimidates or threatens another person or his families with serious danger or injury by disseminating any writing, video, audio or any other image through a computer systems shall be punishable, with simple imprisonment not exceeding three years or in a serious cases with rigorous imprisonment not exceeding five years.

2/ causes fear, threat or psychological strain on another person by sending or by repeatedly transmitting information about the victim or his families through computer system or by keeping the victim's computer communication under surveillance shall be punishable with simple imprisonment not exceeding five years or in serious case with rigorous imprisonment not exceeding 10 years.

3/ disseminates any writing, video, audio or any other image through a computer system that is defamatory to the honor or reputation of another person shall be punishable, upon complaint, with simple imprisonment not exceeding three years or fine or both.

14. Crimes against Public Security

Without prejudice to the provisions Article 257 of the Criminal Code of the Federal Democratic Republic of Ethiopia, Whosoever intentionally disseminates through a computer system any written, video, audio or any other picture that incites fear, violence, chaos or conflict among people shall be punishable with rigorous imprisonment not exceeding three years.

15. Dissemination of Spam

1/ Whosoever, with intent to advertise or sell any product or service, disseminates messages to multiple e-mail addresses at a time shall be punishable with simple imprisonment not exceeding three years and fine or, in serious case, with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.

2/ Notwithstanding the provision of sub-article (1) of this Article, dissemination of commercial advertisement through email account shall not be punishable provided that:

a) there is prior consent from the recipient;

b) the primary purpose of the advertisement is to introduce customers with new products or services and the customers have willing; or

c) the advertisement contains valid identity and address of the sender, and valid and simple way for the recipient to reject or unsubscribe receipt of further advertisement from the same source.

16. Criminal Liability of Service Providers

A service provider shall be criminally liable in accordance with Articles 12 to 14, of this Proclamation for any illegal computer content data disseminated through its computer systems by third parties, if it has:

1/ directly involved in the dissemination or edition of the content data;

2/ upon obtaining actual knowledge that the content data is illegal, failed to take any measure to remove or to disable access to the content data; or

3/ failed to take appropriate measure to remove or to disable access to the content data upon obtaining notice from competent administrative authorities.

SECTION FOUR
OTHER OFFENCES

17. Failure to Cooperate and Hindrance of Investigation

Whosoever:

1/ fails to comply with the obligations provided for under sub-article (2) of Article 23, sub-article (6) of Article 24, sub-article (2) of Article 29, sub-article (2) of Article 30 or sub-article (4) of Article 31 of this Proclamation, shall be punishable with simple imprisonment not exceeding one year or fine;

2/ intentionally hinders the investigation process of computer crimes conducted pursuant to this Proclamation shall be punishable with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000.

18. Criminal Act Stipulated in Other Laws

Where any crime other than those provided for under this Part is committed by means of a computer, the relevant law shall apply.

19. Concurrent Crimes

Where any of the criminal acts provided for under this Part has resulted in the commission of another crime punishable under any special law or criminal code, the relevant provision shall apply concurrently.

20. Penalty Imposed on Juridical Person

Notwithstanding sub-article (1), (3) and (4) of Article 90 of the Criminal Code of the Federal Democratic Republic of Ethiopia, where any offence stipulated under this Part is committed by juridical person,

1/ the penalty shall be fine from Birr 50,000 to 500,000 for a crime punishable with fine;

2/ when the penalty provided for is imprisonment, the penalty shall be:

a) a fine not exceeding 50,000 Birr for a crime punishable with simple imprisonment not exceeding three years,

b) a fine not exceeding 100,000 Birr for a crime punishable with simple imprisonment not exceeding five years,

c) a fine not exceeding 150,000 Birr for a crime punishable with rigorous imprisonment not exceeding five years,

d) a fine not exceeding 200,000 Birr for a crime punishable with rigorous imprisonment not exceeding 10 years,

e) a fine of up to the general maximum laid down in sub-article (1) of this Article for a crime punishable with rigorous imprisonment exceeding 10 years.

3/ Where fine is expressly provided as punishment for a crime, it shall be five fold.

PART THREE
PREVENTIVE AND INVESTIGATIVE MEASURES

21. General

1/ Computer crime prevention and investigation shall be conducted in accordance with the provisions of this Part.

2/ Without prejudice the provisions of this Part, for issues not clearly covered in this law, the provisions of the Criminal Code and other relevant laws shall be applicable to computer crimes.

22. Investigative Power

1/ The public prosecutor and police shall have joint power to investigate criminal acts provided for in this Proclamation. And the public prosecutor shall lead the investigation process.

2/ Where requested to support the investigation process, the Agency shall provide technical support, conduct analysis on collected information, and provide evidences if necessary.

23. Retention of Computer Data

1/ Without prejudice to any provision stipulated in other laws, any service provider shall retain the computer data disseminated through its computer

systems or data relating to data processing or communication service for at least one year.

2/ The data shall be kept in secret unless a court or public prosecutor orders for disclosure.

24. Real-time Collection of Computer Data

Without prejudice special provisions stipulated under other laws,

1/ to prevent computer crimes and collect evidence related information, the investigatory organ may, request court warrant to intercept in real-time or conduct surveillance, on computer data, data processing service, or internet and other related communications of suspects, and the court shall decide and determine a relevant organ that could execute interception or surveillance as necessary.

2/ Sub-article (1) of this Article shall only be applicable when there is no other means readily available for collecting such data and this is approved and decided by the Minister.

3/ Notwithstanding the provisions of sub-article (1) and (2) of this Article, the Minister may give permission to the investigatory organ to conduct interception or surveillance without court warrant where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is or to be committed.

4/ The Minister shall present the reasons for interception or surveillance without court warrant under sub-article (3) of this Article to the President of the Federal High Court within 48 hours, and the president shall give appropriate order immediately.

5/ Unless believed that it is necessary to conduct other criminal investigation, any irrelevant information collected pursuant to sub-articles (1) to (4) of this Article shall be destroyed immediately upon the decision of the Minister.

6/ Any service provider shall cooperate when requested to carry on activities specified under sub-articles (1) and (3) of this Article.

7/ Without prejudice sub-article (5) of this Article, any information collected in accordance with this Article shall be kept confidential.

25. Protection of Computer, Computer System or Infrastructure from Danger

1/ Where there are reasonable grounds to believe that a computer crime is to be committed and it is necessary to prevent and control the crime, provide early warning to citizens, to minimize the risks or for effectiveness of the investigation, the Agency in collaboration with the investigatory organ, may conduct sudden searches, conduct digital forensic investigation, provide appropriate security equipment or take other similar measures on

computers, computer systems or infrastructures that are suspected to be attacked or deemed to be the sources of attack.

2/ For the implementation of the provision of sub-article (1) of this Article, as may be necessary and upon request, concerned organs shall have duty to cooperate.

26. Duty to Report

1/ Any service provider who has knowledge of the commission of the crimes stipulated in this Proclamation or dissemination of any illegal content data by third parties through the computer system it administers shall immediately notify the Agency, accordingly report to the police about the crime and take appropriate measures.

2/ The Agency may issue a directive as to the form and procedures of reporting.

27. Arrest and Detention

Without prejudice the provisions stipulated in special laws,

1/ where there are reasonable grounds to believe that a computer crime is committed or under commission, police may arrest suspects in accordance with the provisions of the Criminal Procedure Code.

2/ Where the investigation on the person arrested pursuant to sub-article (1) of this Article is not completed, remand may be granted in accordance with the provisions of the Criminal Procedure Code; provided, however, the overall remand period may not exceed four months.

PART FOUR

EVIDENTIARY AND PROCEDURAL PROVISIONS

28. General

1/ Computer crime proceedings and collection of evidence shall be conducted in accordance with the provisions of this Part.

2/ Without prejudice to the provisions of this Part, the General Part provisions of the Criminal Code and the Criminal Procedure Code shall be applicable to computer Crimes.

29. Order for Preservation of Computer Data

1/ Where there are reasonable grounds to believe that a computer data required for computer crime investigation is vulnerable to loss or

modification, the investigatory organ may order, in writing, a person to preserve the specified data under his control or possession.

2/ The person ordered under sub-article (1) of this Article shall immediately take necessary measures to secure the specified computer data and preserve it for three months and keep such order confidential.

3/ The investigatory organ may order only a one-time extension for another three months up on the expiry of the period stipulated under sub-article (2) of this Article.

30. <u>Order for Obtaining of Computer Data</u>

1/ Where a computer data under any person's possession or control is reasonably required for purposes of a computer crime investigation, the investigatory organ may apply to the court to obtain or gain access to that computer data.

2/ If the court is satisfied, it may, without requiring the appearance of the person concerned, order the person who is in possession or control of the specified computer data, to produce it to the investigatory organ or give access to same.

31. <u>Access, Search and Seizure</u>

1/ Where it is necessary for computer crime investigation, the investigatory organ may, upon getting court warrant, search or access physically or virtually any computer system, network or computer data.

2/ Where the investigatory organ reasonably believes that the computer data sought is stored in another computer system and can be obtained by same computer system, the search or access may be extended to that other computer system without requesting separate search warrant.

3/ In the execution of search under sub-article (1) or (2) of this Article, the investigatory organ may:

a) seize any computer system or computer data;

b) make and retain a copy or photograph data obtained through search;

c) maintain the integrity of the relevant stored data by using any technology;

d) render inaccessible the stored data from the computer system on which search is conducted; or

e) recover deleted data.

4/ In the execution of search, the investigatory organ may order any person who has knowledge in the course of his duty about the functioning of the

computer system or network or measures applied to protect the data therein to provide the necessary information or computer data that can facilitate the search or access..

5/ Where the investigatory organ finds the functioning of a computer system or computer data is in violation of the provisions this Proclamation or other relevant laws, it may request the court to order for such computer data or computer system to be rendered inaccessible or restricted or blocked. The court shall give the appropriate order within 48 hours after the request is presented.

6/ Where the search process on juridical person requires the presence of the manager or his agent, the investigatory organ shall take appropriate measure to do so.

32. Admissibility of Evidences

1/ Any document or a certified copy of the document or a certified printout of any electronic record relating to computer data seized in accordance with this Proclamation may be produced as evidence during court proceedings and shall be admissible.

2/ Without prejudice to the admissibility of evidences to be produced in accordance with the Criminal Procedure Code and other relevant laws, any digital or electronic evidence:

a) produced in accordance with this Proclamation; or

b) obtained from foreign law enforcement bodies

shall be admissible in court of law in relation to computer crimes.

33. Authentication

Without prejudice to the authentication of written documents stipulated in other laws, any person who produces evidences provided under Article 32 of this Proclamation in a court proceeding has the burden to prove its authenticity.

34. Original Electronic Document

1/ Any electronic record which is obtained upon proof of the authenticity of the electronic records system or by which the data was recorded or stored shall be presumed original electronic document

2/ Without prejudice to sub-article (1) of this Article, the electronic printout which is obtained using a secured system under regular operation shall be considered original electronic evidence.

3/ Where the authenticity of an electronic record is not proved, any evidence that shows the following fact shall be admissible.

a) the computer system was operating properly or the fact of its not operating properly did not affect the integrity of the electronic record; or

b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the other litigant party seeking to introduce it; or

c) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

35. Presumption of Courts

When assessing the admissibility of evidence in accordance with this Proclamation, the court may have regard to the procedure, standard or manner in which a similar computer system is functioning.

36. Burden of proof

1/ Public prosecutor has the burden of proofing material facts regarding the cases brought to the court in accordance with the standards stipulated in law.

2/ Notwithstanding the provisions of sub-article (1) of this Article, upon proof of basic facts of the case by the public prosecutor if the court believes necessary to shift the burden of proofing to the accused, the court may do so.

PART FIVE
INSTITUTIONS THAT FOLLOW UP CASES OF COMPUTER CRIME

37. Public Prosecutor and Police Following up Cases of Computer Crime

1/ A public prosecutor or investigative officer empowered to follows up computer crime cases in accordance with the powers conferred by law shall have the responsibility to enforce and cause to enforce the provisions of this Proclamation.

2/ Public prosecution office and Police empowered in this Proclamation may organize separate specialized task units when necessary to follow up computer crimes

38. Duty of the Agency

The Agency shall have duty to establish online computer crimes investigation system and provide other necessary investigation technologies.

39. Jurisdiction

1/ The Federal High Court shall have first instance jurisdiction over computer crime stipulated under this Proclamation.

2/ The judicial jurisdictions stipulated under Article 13 and paragraph (b) of sub-article (1) of Article 17 of the Federal Democratic Republic of Ethiopia 2004 Criminal Code shall include computer crimes.

40. Establishment of Executing Task Force

1/ Without prejudice the power of the Agency to lead national cyber security operation as stipulated in other relevant laws, a National Executing Task Force comprising the heads of the Ministry of Justice, the Federal Police Commission and other relevant bodies shall be established in order to prevent and control computer crimes.

2/ The Minister of Ministry of Justice shall lead the Executing Task Force, identify other relevant organizations to be incorporated in the Task Force and ensure their representation.

3/ The Task Force shall, for the prevention and control computer crimes, develop national discussion forum, discuss on occasional dangers materialized and provide recommendation thereof, design short and long term plans to be performed by the respective institutions as well as put in place synchronized system by coordinating various relevant organs.

PART SIX
MISCELLANEOUS PROVISIONS

41. International Cooperation

1/ The Ministry of Justice shall cooperate and may sign agreements with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, extradition and other assistances in accordance with this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system.

2/ For the implementation of this Proclamation, the investigatory organ, when necessary, may exchange information, perform joint cooperation in other forms or sign agreement with institutions of another country having similar mission.

3/ Any information or evidence obtained pursuant to this Article shall apply for the purpose of prevention or investigation of computer crimes.

42. Suspension, Confiscation or Blockage of Computer System or Asset

1/ The court, in sentencing an offender under this Proclamation, may give additional order for the suspension, confiscation or removal of any computer system, data or device or blockage of data processing service used in the perpetration of the offence.

2/ The property or proceedings of the accused that he directly or indirectly acquired through the computer crime for which he has been convicted shall be confiscate if the accused is convicted through a final decision;

3/ Unless they are contradictory to the provisions of this Proclamation, the relevant provisions of the Revised Anti-Corruption Special Procedure and Rules of Evidence Proclamation No. 434/2005 (as amended) shall be applicable with respect to restraining or forfeiture order of computer system, data, equipment or other assets.

43. Repeal and Inapplicable Laws

1/ Articles 706 to 711 of the Criminal Code of the Federal Democratic Republic of Ethiopia and article 5 of Telecom Fraud Offence proclamation no. 761/2012 are hereby repealed.

2/ No proclamation, regulations, directives or practices shall, in so far as they are inconsistent with this Proclamation, be applicable with respect to matters provided for by this Proclamation.

44. Effective Date

This Proclamation shall enter into force on the date of its publication in the Federal Negarit Gazeta.

Done at Addis Ababa, this----------day of ----------, 2016

MULATU TESHOME (Dr.)

PRESIDENT OF THE FEDERAL DEMOCRATIC REPUBLIC OF ETHIOPIA