CYBERSECURITY ACT, 2020

Act 1038

ARRANGEMENT OF SECTIONS

Preliminary

Section

REPUBLIC OF GHANA

THE ONE THOUSAND AND THIRTY-EIGHTH

ACT

OF THE PARLIAMENT OF THE REPUBLIC OF GHANA

ENTITLED

CYBERSECURITY ACT, 2020

AN ACT to establish the Cyber Security Authority; to regulate cybersecurity activities in the country; to promote the development of cybersecurity in the country and to provide for related matters.

DATE OF ASSENT: *29th December, 2020.*

PASSED by Parliament and assented to by the President

Preliminary

Application

1. (1) This Act applies to cybersecurity activities in the country.

(2) This Act shall be read together with other relevant enactments including the

(a) Criminal Offences Act, 1960 (Act 29);
(b) Evidence Act, 1975 (N.R.C.D. 323);
(c) Foreign Exchange Act, 2006 (Act 723);
(d) Anti-Money Laundering Act, 2008 (Act 749);
(e) Anti-Terrorism Act, 2008 (Act 762);
(f) Electronic Transactions Act, 2008 (Act 772);
(g) Electronic Communications Act, 2008 (Act 775);
(h) Economic and Organised Crime Office Act, 2010 (Act 804);

(i) Mutual Legal Assistance Act, 2010 (Act 807);
(j) Data Protection Act, 2012 (Act 843); and
(k) Payment Systems and Services Act, 2019 (Act 987).

Cyber Security Authority

Establishment of the Cyber Security Authority

2. (1) There is established by this Act the Cyber Security Authority as a body corporate.

(2) For the performance of functions, the Authority may acquire and hold property, dispose of property and enter into a contract or any other related transaction.

(3) Where there is a hindrance to the acquisition of land, the land may be acquired for the Authority under the State Lands Act, 1962 (Act 125) and the cost shall be borne by the Authority.

Objects of the Authority

3. The objects of the Authority are to

(a) regulate cybersecurity activities in the country;
(b) prevent, manage and respond to cybersecurity threats and cybersecurity incidents;
(c) regulate owners of critical information infrastructure in respect of cybersecurity activities, cybersecurity service providers and practitioners in the country;
(d) promote the development of cybersecurity in the country to ensure a secured and resilient digital ecosystem;
(e) establish a platform for cross-sector engagement on matters of cybersecurity for effective co-ordination and co-operation between key public institutions and the private sector;
(f) create awareness of cybersecurity matters; and
(g) collaborate with international agencies to promote the cybersecurity of the country.

Functions of the Authority

4. To achieve the objects under section 3, the Authority shall

(a) advise the Government and public institutions on all matters related to cybersecurity in the country;
(b) promote the security of computers and computer systems in the country;

(c) monitor cybersecurity threats within and outside the country;

(d) establish codes of practice and standards for cybersecurity, and monitor compliance with the codes of practice and standards by the public and private sector owners of critical information infrastructure;

(e) establish standards for certifying cybersecurity products or services;

(f) certify cybersecurity products or services in accordance with the standards established pursuant to paragraph *(e);*

(g) take measures in response to cybersecurity incidents that occur within and outside the country which may threaten

(i) national security;

(ii) the defence of the country;

(iii) the economy of the country;

(iv) international relations between the State and other countries;

(v) health of the public;

(vi) the safety of life and property; and

(vii) any other sector of the country likely to be affected by a cybersecurity incident;

(h) identify and designate critical information infrastructure and advise the Minister on the regulation of owners of critical information infrastructure to protect the critical information infrastructure of the country, in accordance with international best practice;

(i) provide technical support for law enforcement agencies and security agencies to prosecute cyber offenders;

(j) promote the protection of children online;

(k) issue licences for the provision of cybersecurity services specified in the First Schedule;

(l) establish standards for the provision of cybersecurity services specified in the First Schedule;

(m) support technological advances and research and development in cybersecurity to ensure a resilient and sustainable digital ecosystem;
(n) deploy strategies to implement research findings towards the promotion of the cybersecurity of the country;
(o) establish and maintain a framework for disseminating information on cybersecurity;
(p) submit periodic reports on the state of cybersecurity in the country to the Minister;
(q) educate the public on matters related to cybercrime and cybersecurity;
(r) build the capacity of persons in the public or private sector in matters related to cybersecurity;
(s) collaborate with law enforcement agencies to intercept or disable a digital technology service or product whose operation undermines the cybersecurity of the country;
(t) establish and maintain a national register of
(i) identified and potential risks;
(ii) the levels and impact of risks;
(iii) owners of critical information infrastructure; and
(iv) any other persons licensed or accredited to carry out cybersecurity activities; and
(u) perform any other functions which are ancillary to the objects of the Authority.

Governance of the Authority

Governing body of the Authority

5. (1) The governing body of the Authority is a Board consisting of
(a) the Ministers responsible for
(i) Communications;
(ii) the Interior;
(iii) National Security; and
(iv) Defence;
(b) the Director-General of the Authority;
(c) three persons from the Industry Forum nominated by the Industry Forum; and

(d) three other persons nominated by the President on the advice of the Minister, at least two of whom are women.

(2) The President shall nominate the Minister as chairperson of the Board.

(3) The chairperson and other members of the Board shall be appointed by the President in accordance with article 70 of the Constitution.

Functions of the Board

6. The Board shall, subject to the provisions of this Act,

(a) have oversight responsibility for the Authority;

(b) be responsible for the strategic direction and policies of the Authority;

(c) manage and disburse the Cybersecurity Fund in accordance with section 30; and

(d) ensure the efficient and effective performance of the functions of the Authority.

Tenure of office of members of the Board

7. (1) A member of the Board shall hold office for a period of four years and is eligible for re-appointment for another term only.

(2) Subsection (1) does not apply to the Director-General.

(3) A member of the Board, other than a member appointed under paragraph *(a)* or *(b)* of subsection (1) of section 5, may, at any time, resign from office in writing addressed to the President through the Minister.

(4) A member of the Board who is absent from three consecutive meetings of the Board without sufficient cause ceases to be a member of the Board.

(5) The President may, by a letter addressed to a member, revoke the appointment of the member.

(6) Where a member of the Board is, for a sufficient reason, unable to act as a member, the Minister shall determine whether the inability may result in the declaration of a vacancy.

(7) Where there is a vacancy

(a) under subsection (3), (4) or (5) or subsection (2) of section 9;

(b) as a result of a declaration under subsection (6); or

(c) by reason of the death of a member,

the Minister shall notify the President of the vacancy and the President shall, subject to section 5, appoint a person to fill the vacancy for the unexpired term.

Meetings of the Board

8. (1) The Board shall meet at least once every quarter for the conduct of business at a time and place determined by the chairperson.

(2) The chairperson shall, at the request in writing of not less than one-third of the membership of the Board, convene an extraordinary meeting of the Board, at a time and place determined by the chairperson.

(3) The chairperson shall preside at meetings of the Board and in the absence of the chairperson, a member of the Board, other than the Director-General, elected by the members present from among their number shall preside.

(4) The quorum at a meeting of the Board is seven members of the Board.

(5) Matters before the Board shall be decided by the majority of the members present and voting and in the event of an equality of votes, the person presiding shall have a casting vote.

(6) The Board may co-opt a person to attend a meeting of the Board but that person shall not vote on any matter for decision at the meeting.

(7) The validity of any proceedings of the Board shall not be affected by a vacancy among the members of the Board or by a defect in the appointment or qualification of a member.

(8) The Board shall, subject to this section, regulate the procedure for the meetings of the Board.

Disclosure of interest

9. (1) A member of the Board who has an interest in a matter for consideration by the Board

(a) shall disclose in writing the nature of that interest and the disclosure shall form part of the record of the consideration of the matter; and

(b) is disqualified from being present at or participating in the deliberations of the Board in respect of that matter.

(2) Where a member contravenes subsection (1), the chairperson shall inform the President in writing to revoke the appointment of the member.

(3) Without limiting any further cause of action that may be instituted against the member, the Board shall recover any benefit derived by a member who contravenes subsection (1).

Establishment of committees

10. (1) The Board may establish committees consisting of members of the Board and non-members or both, to perform a function of the Board.

(2) A committee of the Board composed of members and non-members shall be chaired by a member of the Board.

(3) A committee of the Board composed of non-members only shall be advisory.

(4) Section 9 applies to a member of a committee of the Board.

Allowances

11. Members of the Board and members of a committee of the Board shall be paid allowances determined by the Minister in consultation with the Minister responsible for Finance.

Policy directives

12. To achieve the object of this Act, the Minister may give directives in writing on matters of policy to the Board and the Board shall comply.

Joint Cybersecurity Committee

13. (1) There is established by this Act a Joint Cybersecurity Committee.

(2) The Joint Cybersecurity Committee consists of

(a) a Justice of the Superior Court of Judicature with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Chief Justice;

(b) the Director-General of the National Information Technology Agency or a representative of the Director-General with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Director-General;

(c) the Director-General of the National Communications Authority or a representative of the Director-General with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Director-General;

(d) the Executive Director of the Data Protection Commission or a representative of the Executive Director with the

requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Executive Director;

(e) the Governor of the Bank of Ghana or a representative of the Governor with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Governor;

(f) the Chief Executive Officer of the Financial Intelligence Centre or a representative of the Chief Executive Officer with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Chief Executive Officer;

(g) the Director of the Bureau of National Investigations or a representative of the Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Director;

(h) the Executive Director of the Economic and Organised Crime Office or a representative of the Executive Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Executive Director;

(i) the Director-General of the Criminal Investigation Department of the Ghana Police Service or a representative of the Director-General with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Inspector-General of Police;

(j) the Director of Operations of the National Security Council Secretariat or a representative of the Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Head of the National Security Council Secretariat;

(k) the Director of the Bureau of National Communications or a representative of the Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Director;

(l) the Director-General of Defence Intelligence or a representative of the Director-General with the requisite

knowledge and skills in cybercrime and cybersecurity matters, nominated by the Chief of Defence Staff;

(m) the Comptroller-General of the Immigration Service or a representative of the Comptroller-General with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Comptroller-General;

(n) the Director of External Intelligence or a representative of the Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Chief of Defence Staff;

(o) a representative of the Ghana Armed Forces not below the rank of a Colonel with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Chief of Defence Staff;

(p) the Director of the Public Prosecutions Division of the Office of the Attorney-General or a representative of the Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Attorney-General;

(q) the Director-General of the Authority; and

(r) the Executive Director of the Ghana Domain Name Registry or a representative of the Executive Director with the requisite knowledge and skills in cybercrime and cybersecurity matters, nominated by the Executive Director.

(3) A nomination under subsection (2) shall be made in consultation with the Authority.

(4) The President shall appoint the members of the Joint Cybersecurity Committee.

(5) The Director-General of the Authority shall preside at meetings of the Joint Cybersecurity Committee and in the absence of the Director-General, a member of the Committee elected by the members present from among the number shall preside.

(6) The Joint Cybersecurity Committee shall meet at a time and place determined by the Director-General.

(7) The quorum at a meeting of the Joint Cybersecurity Committee is ten members.

(8) Matters before the Joint Cybersecurity Committee shall be decided by a majority of the members present and voting and in the event of an equality of votes, the person presiding shall have a casting vote.

(9) The Joint Cybersecurity Committee shall regulate the procedure for meetings of the Committee.

(10) Members of the Joint Cybersecurity Committee shall be paid allowances determined by the Minister in consultation with the Minister responsible for Finance.

(11) The Joint Cybersecurity Committee may establish sub-committees comprising members of the Joint Cybersecurity Committee and non-members, including representatives from the private sector, to perform a function of the Joint Cybersecurity Committee.

(12) A sub-committee established under subsection (10) shall meet regularly for the conduct of business where the exigencies require.

(13) The Joint Cybersecurity Committee shall have a Secretariat at the Headquarters of the Authority.

Functions of the Joint Cybersecurity Committee

14. (1) The Joint Cybersecurity Committee shall collaborate with the Authority and the sectors or institutions represented on the Committee for the implementation of relevant cybersecurity measures.

(2) The Joint Cybersecurity Committee is answerable to the Board in the performance of functions of office.

Administrative Provisions

Appointment of Director-General

15. (1) The President shall, in accordance with article 195 of the Constitution, appoint a Director-General for the Authority.

(2) The Director-General shall hold office on the terms and conditions specified in the letter of appointment.

(3) A person is qualified for appointment as a Director-General if that person

(a) has the relevant qualifications and expertise in cybersecurity matters; and

(b) is a person of proven integrity.

Functions of the Director-General

16. (1) The Director-General is responsible for the day-to-day administration and management of the Authority and is answerable to the Board in the performance of functions under this Act.

(2) The Director-General is responsible for the implementation of the decisions of the Board.

(3) The Director-General may delegate a function to an officer of the Authority but shall not be relieved of the ultimate responsibility for the performance of the delegated function.

Secretary to the Board

17. (1) The Authority shall designate a person appointed under section 20 as the Secretary to the Board.

(2) A person shall not be engaged as Secretary to the Board unless that person has

(a) a professional qualification that equips that person with the requisite knowledge and experience to perform the functions under subsection (3); or

(b) by virtue of an academic qualification, or as a member of a professional body, is considered by the Board as capable of performing the functions of the Secretary.

(3) The Secretary shall subject to the directives of the Board

(a) arrange the business of the Board;

(b) keep the minutes of the meetings and decisions of the Board in the form required by the Board; and

(c) perform any other functions that the Board or the Director-General may direct.

(4) The Secretary is answerable to the Board in the performance of the functions of office.

Appointment of inspectors

18. (1) The President shall appoint inspectors for the Authority.

(2) An inspector shall hold office on the terms and conditions specified in the letter of appointment and the emoluments of the inspector shall be charged on the funds of the Authority.

(3) A person is qualified for appointment as an inspector if that person

(a) has knowledge and background in technology and cybersecurity; and

(b) is a person of proven integrity.

(4) Despite subsection (1), an inspector appointed under this Act is not subject to the direction or control of a person or any authority in the performance of functions under this Act.

Functions of inspectors

19. (1) An inspector shall

(a) ensure that a production order or an interception warrant issued under this Act is used for the purpose for which the order or warrant was issued;

(b) ensure that data retained or retrieved in accordance with this Act is used for the purpose for which that data was retained or retrieved; and

(c) submit quarterly reports on the outcome of inspections carried out to the Board.

(2) The expenses incurred in the performance of the functions of an inspector shall be charged on the funds of the Authority.

(3) An inspector is answerable to the Board in the performance of the functions of office.

Appointment of other staff

20. (1) The President shall, in accordance with article 195 of the Constitution, appoint any other staff of the Authority that are necessary for the efficient and effective performance of the functions of the Authority.

(2) Other public officers may be transferred or seconded to the Authority or may give assistance to the Authority.

(3) The Authority may, for the efficient and effective discharge of the functions of the Authority, engage the services of consultants and advisors on the recommendation of the Board.

Divisions of the Authority

21. (1) The Board may establish divisions of the Authority that are necessary for the efficient and effective performance of the functions of the Authority.

(2) A division of the Authority shall be headed by a director.

Internal Audit Unit

22. (1) The Authority shall have an Internal Audit Unit in accordance with section 83 of the Public Financial Management Act, 2016 (Act 921).

(2) The Internal Audit Unit shall be headed by an Internal Auditor who shall be appointed in accordance with the Internal Audit Agency Act, 2003 (Act 658).

(3) The Internal Auditor is responsible for the internal audit of the Authority.

(4) The Internal Auditor shall, subject to subsections (3) and (4) of section 16 of the Internal Audit Agency Act, 2003 (Act 658), at intervals of three months

(a) prepare and submit to the Board, a report on the internal audit carried out during the period of three months immediately preceding the preparation of the report; and

(b) make recommendations in each report, with respect to matters which appear to the Internal Auditor as necessary for the conduct of the affairs of the Authority.

(5) The Internal Auditor shall, in accordance with subsection (4) of section 16 of the Internal Audit Agency Act, 2003 (Act 658), submit a copy of each report prepared under this section to the Director-General and the chairperson of the Board.

Financial Provisions

Funds of the Authority

23. The funds of the Authority include

(a) moneys approved by Parliament;

(b) administrative penalties;

(c) any other internally generated funds;

(d) loans, grants and donations approved by the Minister responsible for Finance;

(e) an amount charged on the Fund subject to the approval of the Board; and

(f) any other moneys approved by the Minister responsible for Finance.

Bank account of the Authority

24. The moneys for the Authority shall be paid into a bank account opened for the purpose, by the Authority with the approval of the Controller and Accountant-General.

Borrowing powers of the Authority

25. Subject to section 76 of the Public Financial Management Act, 2016, (Act 921), the Authority may obtain loans and any other credit facility on the guarantee of the Government from a bank or any other financial institution approved by the Minister responsible for Finance.

Expenses of the Authority

26. The expenses of the Authority shall be charged on the funds of the Authority.

Accounts and audit

27. (1) The Board shall keep books, records, returns and other documents relevant to the accounts in the form approved by the Auditor-General.

(2) The Board shall submit the accounts of the Authority to the Auditor-General for audit at the end of the financial year.

(3) The Auditor-General shall, within six months after the end of the immediately preceding financial year, audit the accounts and forward a copy each of the audit report to the Minister and the Board.

(4) The financial year of the Authority is the same as the financial year of Government.

Annual report and other reports

28. (1) The Board shall, within thirty days after the receipt of the audit report, submit an annual report to the Minister covering the activities and operations of the Authority for the year to which the annual report relates.

(2) The annual report shall include

(a) the report of the Auditor-General;

(b) a list of persons granted licences and accreditation in the year to which the annual report relates;

(c) the number and outcome of production orders and interception warrants issued under this Act in the year to which the annual report relates; and

(d) the report of an inspector attached as a separate report.

(3) The Minister shall, within thirty days after the receipt of the annual report, submit the report to Parliament with a statement that the Minister considers necessary.

(4) The Board shall submit to the Minister any other report which the Minister may require in writing.

Cybersecurity Fund

Establishment of the Cybersecurity Fund

29. There is established by this Act a Cybersecurity Fund.

Object of the Fund

30. (1) The object of the Fund is to provide financial resources to promote and strengthen the cybersecurity of the country.

(2) To achieve the object of the Fund, moneys from the Fund shall be applied to relevant activities that the Board may determine.

(3) Without limiting subsection (2), moneys from the Fund shall be applied to

(a) support research and development in cybersecurity;

(b) support domestic, regional and international capacity building exercises in cybersecurity initiatives relevant to the cybersecurity of the country; and

(c) undertake any other activity that is ancillary to the object of the Fund.

Sources of moneys for the Fund

31. The sources of moneys for the Fund include

(a) seed money approved by Parliament;

(b) moneys which may become lawfully payable to the Authority for the Fund;

(c) grants, gifts, donations and other voluntary contributions;

(d) a charge determined by the Authority in accordance with the Fees and Charges (Miscellaneous Provisions) Act, 2018 (Act 983) and levied on persons licensed by the Bank of Ghana to carry on business;

(e) a proportion of the fees charged on all government e-services determined by the Authority in accordance with the Fees and Charges (Miscellaneous Provisions) Act, 2018 (Act 983)

(f) a levy that may be imposed by Parliament on e-services; and

(g) any other moneys approved by Parliament for the Fund.

Bank account for the Fund

32. Moneys for the Fund shall be paid into a bank account opened for that purpose by the Authority with the approval of the Controller and Accountant-General.

Management of the Fund

33. (1) The Board is responsible for the management of the Fund.

(2) Sections 27 and 28 on accounts and audit, and annual report and other reports apply to the Fund.

Disbursement from the Fund

34. The moneys from the Fund shall be disbursed in accordance with the policy guidelines of the Fund.

Critical Information Infrastructure

Designation of critical information infrastructure

35. (1) The Minister may, on the advice of the Authority, designate a computer system or computer network as a critical information infrastructure if the Minister considers that the computer system or computer network is essential for

(a) national security, or

(b) the economic and social well-being of citizens.

(2) Where the Minister designates a computer system or computer network as a critical information infrastructure, the Minister shall publish the designation in the *Gazette*.

(3) The Minister shall, in making a determination under subsection (1), consider if the computer system or computer network is necessary for

(a) the security, defence or international relations of the country;

(b) the production, preservation or identity of a confidential source of information related to the enforcement of criminal law;

(c) the provision of services directly related to

(i) communications and telecommunications infrastructure;

(ii) banking and financial services;

(iii) public utilities;

(iv) public transportation; and

(v) public key infrastructure;

(d) the protection of public safety and public health, including systems related to essential emergency services;
(e) an international business or communication affecting a citizen of Ghana or any other international business in which a citizen of Ghana or the Government has an interest; or
(f) the Legislature, Executive, Judiciary, Public Services or security agencies.

(4) The Minister shall, by publication in the *Gazette*, establish the procedure for the regulation of a critical information infrastructure.

Registration of critical information infrastructure

36. (1) The Authority shall register a critical information infrastructure.

(2) The Authority shall, by publication in the *Gazette*, determine
(a) the requirements for the registration of a critical information infrastructure;
(b) the procedure for the registration of a critical information infrastructure; and
(c) any other matter relating to the registration of a critical information infrastructure.

(3) Where there is any change in the legal ownership of a registered critical information infrastructure, the owner of the registered critical information infrastructure shall, within seven days after the change, inform the Authority of the change in ownership.

(4) An owner of a registered critical information infrastructure who contravenes subsection (3) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Withdrawal of designation of critical information infrastructure

37. The Minister may, on the advice of the Authority and by publication in the *Gazette*, withdraw the designation of a critical information infrastructure at any time if the Minister considers that the computer system or computer network no longer satisfies the criteria of a critical information infrastructure.

Management and compliance audit of critical information infrastructure

38. (1) The Minister shall prescribe minimum standards for prohibitions in respect of the general management of a critical information

infrastructure that the Minister considers necessary for the protection of national security.

(2) The Authority shall carry out a periodic audit and inspection on a critical information infrastructure to ensure compliance with the provisions of this Act.

Duty of owner of critical information infrastructure

39. (1) An owner of a critical information infrastructure shall

(a) report a cybersecurity incident within twenty-four hours after the incident is detected to

(i) the relevant Sectoral Computer Emergency Response Team, or

(ii) the National Computer Emergency Response Team, in the case of a critical information infrastructure that does not belong to a Sectoral Computer Emergency Response Team;

(b) cause an audit to be performed on a critical information infrastructure; and

(c) submit a copy of the audit report to the Authority.

(2) An owner of a critical information infrastructure who contravenes

(a) paragraph *(a)* of subsection (1),

(b) paragraph *(b)* of subsection (1), or

(c) paragraph *(c)* of subsection (1)

is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Access to critical information infrastructure

40. (1) A person shall not without authorisation

(a) secure access, or

(b) attempt to secure access

to a computer system or a computer network designated as a critical information infrastructure.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not less than two thousand, five hundred penalty units and not more than fifteen thousand

penalty units or to a term of imprisonment of not less than two years and not more than five years, or to both.

(3) Where the offence committed under subsection (1)

(a) results in a serious bodily injury, financial loss or damage to the computer system or computer network designated as a critical information infrastructure, the person who commited the offence

(i) in the case of an individual, is liable on summary conviction to a fine of not less than five thousand penalty units and not more than fifty thousand penalty units or to a term of imprisonment of not less than five years and not more than fifteen years or to both; or

(ii) in the case of a body corporate, a partnership or a firm is liable on summary conviction to a fine of not less than twenty-five thousand penalty units and not more than fifty thousand penalty units; and

(b) is deemed to be a terrorist act, the person who committed the offence is liable on conviction on indictment to a term of imprisonment of not less than seven years and not more than twenty-five years.

(4) Where an offence under subsection (3) is committed by a body corporate or by a member of a partnership or other firm, every director or officer of that body corporate or a member of the partnership or any other person concerned with the management of the firm shall be deemed to have committed that offence and is liable on summary conviction to a fine of not less than five thousand penalty units and not more than fifty thousand penalty units.

(5) A person shall not be convicted of an offence by virtue of subsection (4) if it is proved that

(a) due diligence was exercised to prevent the commission of the offence; and

(b) the offence was committed without the knowledge, consent or connivance of that person.

National and Sectoral Computer Emergency Response Teams

Establishment of the National Computer Emergency Response Team

41. There is established by this Act, the National Computer Emergency Response Team.

Functions of the National Computer Emergency Response Team

42. The National Computer Emergency Response Team

(a) is responsible for responding to cybersecurity incidents;

(b) shall co-ordinate responses to cybersecurity incidents amongst public institutions, private institutions and international bodies; and

(c) oversee the Sectoral Computer Emergency Response Team established under section 44.

Responsibility of the Authority relating to response to cybersecurity incident

43. (1) The Authority shall ensure that the National Computer Emergency Response Team

(a) is equipped with the relevant tools required to effectively respond to cybersecurity incidents; and

(b) co-operates with Sectoral Computer Emergency Response Team of other countries in respect of cybersecurity incidents.

(2) The Authority may give regulatory directives to the Sectoral Computer Emergency Response Teams and the Sectoral Computer Emergency Response Teams shall comply.

Sectoral Computer Emergency Response Team

44. (1) For the purposes of achieving an effective cybersecurity incident co-ordination, the Authority shall, by notice published in the *Gazette*, establish Sectoral Computer Emergency Response Teams to

(a) collect and collate cybersecurity incidents; and

(b) co-ordinate responses to cybersecurity incidents within the sectors.

(2) The Authority shall, in establishing a Sectoral Computer Emergency Response Team, take into account factors including

(a) the needs and criticality of a sector; and

(b) developments in respect of cybersecurity in the country.

(3) The establishment and operational cost of a Sectoral Computer Emergency Response Team established under subsection (1) shall be borne by the sector concerned.

(4) The Authority shall accredit and oversee the operation of Sectoral Computer Emergency Response Teams.

(5) A Sectoral Computer Emergency Response Team shall submit to the Authority, through the administrative head of that Sectoral Computer Emergency Response Team, a monthly report covering the operations of that Sectoral Computer Emergency Response Team based on a reporting template determined by the Authority.

(6) A Sectoral Computer Emergency Response Team that fails to comply with the regulatory directives of the Authority, is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

(7) A notice published under subsection (1) shall state the relevant requirements including the

(a) reporting obligation of the Sectoral Computer Emergency Response Team concerned and the penalty for non-compliance; and

(b) adherence to risk management protocols.

(8) For the purposes of this section, "sector" includes the

(a) public sector;

(b) banking and financial sector;

(c) telecommunication sector;

(d) energy and utilities sector;

(e) military sector;

(f) national security sector;

(g) academic sector;

(h) health sector;

(i) transportation sector; and

(j) any other sector determined by the Authority.

Cybersecurity incident monitoring and response system

45. (1) The Authority may establish a cybersecurity incident monitoring and response system.

(2) The Authority shall implement the relevant technical measures to ensure an effective cybersecurity incident monitoring and response system.

(3) Without limiting subsection (2), a technical measure aimed at ensuring an effective cybersecurity incident monitoring and response system shall include an interception capability to execute an interception warrant authorised by a Court.

(4) For the purposes of subsection (3), the Authority shall intercept, disable or take-down a digital technology, digital service or a digital product that is likely to undermine the cybersecurity of the country.

Early warning system

46. (1) The Authority shall establish an early warning system in respect of human initiated risks that are likely to undermine the cybersecurity of the country.

(2) The Authority shall implement the early warning system to advise the public on cybersecurity matters.

Cybersecurity Incident Reporting

Duty to report cybersecurity incident

47. (1) A Sectoral Computer Emergency Response Team shall report a cybersecurity incident to the Authority through the National Computer Emergency Response Team.

(2) An institution licensed by the Authority to provide a cybersecurity service shall, within the period determined by the Authority, submit to the Authority a report covering the operations of that institution including a report of a cybersecurity incident.

(3) The Authority shall establish a cybersecurity incident reporting and information sharing platform to enable a Sectoral Computer Emergency Response Team, a licensee and any other relevant institution report a cybersecurity incident.

(4) The Authority shall, upon receipt of information in respect of a cybersecurity incident, circulate the information to a Sectoral Computer Emergency Response Team, a licensee and any other relevant institution.

(5) A person in charge of an institution shall report a cybersecurity incident to the relevant Sectoral Computer Emergency Response Team or the National Computer Emergency Response Team within a period of not more than twenty-four hours after the incident is detected.

(6) A person who contravenes subsection (5) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Cybersecurity incident point of contact

48. (1) The Authority shall, establish a cybersecurity incident point of contact to facilitate

(a) reporting of a cybersecurity incident by the general public; and

(b) international co-operation in cybersecurity matters.

(2) An institution that is not affiliated to a designated Sectoral Computer Emergency Response Team, shall report a cybersecurity incident to the National Computer Emergency Response Team through the cybersecurity incident point of contact established under subsection (1).

(3) An individual may report a cybersecurity incident to the National Computer Emergency Response Team through the cybersecurity incident point of contact established under subsection (1).

Licensing of Cybersecurity Service Providers

Licensing of cybersecurity service providers

49. (1) A person shall not provide a cybersecurity service unless that person obtains a licence issued by the Authority in accordance with this Act.

(2) A person who contravenes subsection (1) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Application for licence

50. (1) A person who seeks to provide a cybersecurity service shall apply in writing to the Authority.

(2) The application shall be made in the prescribed form and accompanied by the

(a) supporting documentation, and

(b) prescribed fee,

that the Authority may determine.

(3) The Authority shall within fourteen days of receipt of an application, acknowledge receipt of the application.

Grant of licence

51. (1) Where the Authority is satisfied that

(a) the applicant meets the requirements of the Authority for the grant of a licence, and

(b) the grant of a licence is not against public interest

the Authority may grant the licence to the applicant.

(2) The Authority shall, within thirty days of receipt of an application for a licence, inform the applicant in writing of the decision of the Authority.

(3) A licence granted by the Authority is subject to the terms and conditions specified in the licence.

(4) Where the Authority refuses to grant a licence, the Authority shall within twenty-eight days after the refusal communicate in writing the reason for the refusal to grant the licence.

(5) A licensed cybersecurity service provider who uses a licence for a purpose other than that for which the licence was granted is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Non-transferability of licence

52. (1) A person granted a licence shall not transfer that licence to another person.

(2) A person who transfers a licence contrary to subsection (1) commits an offence and is liable on summary conviction to a fine of not less than five thousand penalty units and not more than ten thousand penalty units or to a term of imprisonment of not less than six months and not more than two years, or to both.

Validity and duration of licence

53. (1) A licence granted under this Act is valid for two years from the date that the licence is granted.

(2) A licensed cybersecurity service provider who intends to continue operations as a cybersecurity service provider shall, not later than one month before the expiration of the licence, apply in writing to the Authority for a renewal of the licence.

Suspension of licence

54. (1) The Authority may suspend a licence issued under this Act for a period of not more than six months where

(a) the licensee fails to renew the licence not later than one month before the expiration of the licence; or

(b) the licensee fails to comply with a condition specified in the licence.

(2) The Authority shall, before exercising the power of suspension under this section,

(a) give the licensee thirty days notice in writing of the intention to do so, and

(b) specify in the notice the grounds on which the Authority intends to suspend the licence.

(3) Where the Authority decides to suspend a licence, the Authority shall give the licensee the opportunity

(a) to submit to the Authority, within the time specified by the Authority, a written statement of objections, if any, to the suspension of the licence; and

(b) to remedy, within the time specified by the Authority, the breach which has occasioned the decision to suspend the licence.

(4) The Authority shall, within twenty-eight days of the suspension of a licence, notify the cybersecurity service provider concerned of the suspension.

Revocation of licence

55. (1) The Authority may revoke a licence issued under this Act if the Authority considers that

(a) the licence has been obtained by fraud or misrepresentation;

(b) the licensee has ceased to carry on the business for which the licensee is licensed;

(c) the licensee has been convicted of an offence under this Act or an offence involving fraud, dishonesty or moral turpitude;

(d) a circumstance existed at the time the licence was granted or renewed that the Authority was unaware of, which would have prevented the Authority from granting or renewing the licence of the licensee if the Authority had been aware of the circumstance at that time;

(e) the licensee has been declared bankrupt or has gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction;

(f) the licensee no longer meets the requirements for holding the licence; or

(g) it is not in the public interest for the licensee to continue to carry on the business of a licensee.

(2) Subsections (1) and (2) of section 54 apply to revocation of a licence.

(3) The Authority shall publish the revocation of a licence under this section in the *Gazette*.

Review of decision of Authority

56. (1) A person aggrieved by a decision of the Authority may, within twenty-eight days of receipt of the decision, submit a complaint in writing to the Board for a review of the decision.

(2) A person dissatisfied with the decision of the Board may, within twenty-eight days after the date of receipt of the decision, submit a complaint in writing to the Minister for a review of the decision of the Board.

(3) A person dissatisfied with the decision of the Minister may, within twenty-eight days after the date of receipt of the decision, seek redress in a court of competent jurisdiction.

Accreditation and Certification

Accreditation of cybersecurity professionals and practitioners

57. The Authority shall establish a mechanism for the accreditation of cybersecurity professionals and practitioners.

Certification of cybersecurity products and technology solutions

58. The Authority shall establish a mechanism for the certification of cybersecurity products and technology solutions.

Cybersecurity Standards, Enforcement and Education

Cybersecurity standards and enforcement

59. (1) The Authority shall develop, establish and adopt standards for cybersecurity

(a) education and skills development;
(b) hardware and software engineering;
(c) governance and risk management;
(d) research and development; and
(e) practitioners in any other relevant area that the Authority may determine in accordance with international best practice.

(2) The Authority shall publish on the website of the Authority, the standards developed and promote the adoption of the standards by a

Sectoral Computer Emergency Response Team, a licensed service provider, an institution or any other relevant person.

(3) The Authority shall take the necessary measures to enforce the cybersecurity standards adopted and monitor compliance by the public and private sectors with the cybersecurity standards.

(4) A person who breaches the cybersecurity standards is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Cybersecurity public awareness and education

60. The Authority shall carry out programmes to promote public awareness and education on matters relating to cybersecurity.

Research and development programme

61. The Authority shall

(a) develop and implement a research and development programme to promote the development of cybersecurity in the country;

(b) develop a qualification and competency framework for

(i) persons offering training in cybersecurity programmes; and

(ii) educational institutions offering cybersecurity programmes;

(c) develop or implement technology solutions to mitigate existing and emerging cybersecurity threats and vulnerabilities to ensure the cybersecurity of the country; and

(d) collaborate with academic research centres and other relevant institutions within and outside the country, for the development and implementation of cybersecurity research and development programmes for the country.

Protection of Children Online

Indecent image or photograph of a child

62. (1) A person shall not

(a) take or permit to be taken an indecent image or photograph of a child;

(b) produce or procure an indecent image or photograph of a child for the purpose of the publication of the indecent image or photograph through a computer system;

(c) publish, stream, including live stream, an indecent image or photograph of a child through a computer or an electronic device; or

(d) possess an indecent image or photograph of a child in a computer system or on a computer or electronic record storage medium.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of not less than two thousand five hundred penalty units and not more than five thousand penalty units or to a term of imprisonment of not less than five years and not more than ten years or to both.

(3) For purposes of paragraph *(c)* of subsection (1), a person publishes an indecent photograph, image or visual recording if that person,

(a) parts with possession of the indecent photograph, image or recording to another person; or

(b) exposes or offers the indecent photograph, image or recording for acquisition by another person.

(4) For the purpose of this section, "indecent image or photograph" includes a material image, visual recording, video, drawing or text that depicts

(a) a child engaged in sexually explicit or suggestive conduct;

(b) a person who appears to be a child engaged in sexually explicit or suggestive conduct;

(c) images representing a child engaged in sexually explicit or suggestive conduct;

(d) sexually explicit images of children;

(e) any written material, visual representation or audio recording that advocates or counsels sexual activity with children that would be an offence under the Criminal Offences Act, 1960 (Act 29) or any other relevant enactment;

(f) any written material that has, as its dominant characteristic, the description, for a sexual purpose, of sexual activity with a child that would be an offence under the Criminal Offences Act, 1960 (Act 29) or any other relevant enactment; or

(g) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a child that would be an offence under the Criminal Offences Act, 1960 (Act 29) or any other relevant enactment.

Dealing with a child for purposes of sexual abuse

63. (1) A person shall not use

(a) a computer online service,

(b) an internet service,

(c) a local bulletin board service, or

(d) any other device capable of electronic data storage or transmission

to seduce, solicit, lure, groom or entice, or attempt to seduce, solicit, lure, groom or entice, a child or another person believed by the person to be a child, for the purpose of facilitating, encouraging, offering, or soliciting unlawful sexual conduct of or with any child, or the visual depiction of such conduct.

(2) A person who contravenes subsection (1), commits an offence and is liable on summary conviction to a term of imprisonment of not less than five years and not more than fifteen years.

Aiding and abetting of child dealing for purposes of sexual abuse

64. (1) An owner or operator of a computer on-line service, weblog, internet service, or internet bulletin board service shall not

(a) aid and abet another person for the purpose of facilitating or encouraging the on-line solicitation of a child; or

(b) permit any person to use the service of that person for the purpose of facilitating, encouraging, offering, or soliciting unlawful sexual conduct of or with a child, or the visual depiction of such conduct.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than five years and not more than fifteen years.

Cyberstalking of a child

65. (1) A person shall not use a computer online service, an internet service, or a local internet bulletin board service or any other electronic device to compile, transmit, publish, reproduce, buy, sell, receive, exchange, or disseminate the name, telephone number, electronic mail address, residence address, picture, physical description, characteristics, or any other identifying information on a child in furtherance of an effort to arrange a meeting with the child for the purpose of engaging in sexual intercourse, sexually explicit conduct, or unlawful sexual activity.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than five years and not more than fifteen years.

(3) For the purpose of this section, "unlawful sexual activity" means a sexual activity characterised by

(a) a recurrent intense sexual urge of a person,

(b) a sexually arousing fantasy of a person, or

(c) the use of an object by a person

resulting in the suffering or humiliation of that person, the partner of that person, a child or any other non-consenting partner.

Sexual extortion

66. (1) A person shall not threaten to distribute by post, email, text, or transmit, by electronic means or otherwise, a private image or moving images of the other person engaged in sexually explicit conduct, with the specific intent to

(a) harass, threaten, coerce, intimidate or exert any undue influence on the person, especially to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or

(b) actually extort money or other consideration or compel the victim to engage in unwanted sexual activity.

(2) A person shall not threaten to distribute by post, email, text, or transmit, by electronic means or otherwise, an intimate image of a child engaged in sexually explicit conduct, with the specific intent to

(a) harass, threaten, coerce, or intimidate the person, especially with intent to extort money or other consideration or to compel the victim to engage in unwanted sexual activity; or

(b) actually extort money or other consideration or compel the victim to engage in unwanted sexual activity.

(3) For the purposes of subsections (1) and (2), an intimate image may include a depiction in a way that the genital or anal region of another person is bare or covered only by underwear; or the breasts below the top of the areola, that is either uncovered or clearly visible through clothing.

(4) A person who contravenes subsection (1) or (2) commits an offence and is liable on summary conviction to a term of imprisonment of not less than ten years and not more than twenty five years.

Other Online Sexual Offences

Non-consensual sharing of intimate image

67. (1) A person shall not, with intent to, cause serious emotional distress, intentionally distribute or intentionally cause another person to distribute the intimate image or prohibited visual recording of another identifiable person without the consent of the person depicted in the intimate image and in respect of which, there was a reasonable expectation of privacy both at the time of the creation of the image or visual recording and at the time the offence was committed.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than one year and not more than three years.

(3) For the purpose of this section, "serious emotional distress" includes any intentional conduct that results in mental reactions such as fright, nervousness, grief, anxiety, worry, mortification, shock, humiliation and indignity, as well as physical pain.

Threat to distribute prohibited intimate image or visual recording

68. (1) A person shall not threaten another person to distribute a prohibited intimate image or visual recording of that person in a way that would cause that other person distress reasonably arising in all the circumstances and the threat is made in a way that would cause that other person fear, reasonably arising in all the circumstances, of the threat being carried out.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a term of imprisonment of not less than one year and not more than three years.

Cybersecurity and Investigatory Powers

Application for production order of subscriber information

69. (1) An investigative officer may apply ex-parte to the High Court, for a production order to collect subscriber information.

(2) An investigative officer who makes an application under subsection (1) shall demonstrate to the satisfaction of the Court that there are reasonable grounds to believe that the subscriber information associated with a specified communication and related to or connected with a person under investigation is reasonably required for the purposes of a specific criminal investigation.

(3) Where an investigative officer makes an application under subsection (1), that investigative officer shall

(a) explain why the investigative officer believes the subscriber information sought, will be available to the person in control of the computer or computer system;

(b) identify and explain with specificity the type of subscriber information suspected to be found on the computer or computer system;

(c) identify and explain with specificity the subscribers, users or unique identifier that may be found on a computer or computer system that is the subject of an investigation or prosecution;

(d) identify and explain with specificity the offences in respect of which the production order is sought; and

(e) indicate what measures shall be taken to ensure that the subscriber information will be procured

(i) whilst maintaining the privacy of other users, customers and third parties, and

(ii) without the disclosure of the subscriber information of any party not part of the investigation.

(4) Subject to clause (14) of article 19 of the Constitution, proceedings under this section and sections 65 and 68 shall be held in camera.

Issue of production order for subscriber information

70. (1) The High Court may grant an application for a production order under section 69 if the Court is satisfied that

(a) the investigative officer has complied with subsections (2) and (3) of section 69;

(b) the information requested is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

(c) measures shall be taken to ensure that the subscriber information is produced whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and

(d) the investigation may be frustrated or seriously prejudiced unless the production of the information is permitted.

(2) The Court shall require the service provider to keep confidential the production order and execution of the production order under this section.

(3) A production order granted under this section shall be served on a domestic service provider, foreign service provider or both.

(4) A service provider that contravenes subsection (2) commits an offence and is liable on summary conviction to a fine of not less than ten thousand penalty units and not more than twenty thousand penalty units.

Application for interception of traffic data

71. (1) A senior investigative officer authorised by a designated officer may apply ex-parte to the High Court, for an interception warrant to collect or record traffic data stored or in real-time.

(2) A senior investigative officer authorised by a designated officer who makes an application under subsection (1) shall demonstrate to the

satisfaction of the Court that there are reasonable grounds to believe that traffic data associated with a specified communication and related to or connected with a person under investigation is reasonably required for the purposes of a specific criminal investigation.

(3) Where a senior investigative officer authorised by a designated officer makes an application under subsection (1), that senior investigative officer shall

(a) explain why the senior investigative officer believes traffic data sought, will be available to the person in control of the computer or computer system;

(b) identify and explain with specificity the type of traffic data suspected to be found on the computer or computer system;

(c) identify and explain with specificity the subscribers, users or unique identifier that may be found on a computer or computer system that is the subject of an investigation or prosecution;

(d) identify and explain with specificity the offences in respect of which the interception warrant is sought; and

(e) indicate what measures shall be taken to ensure that the traffic data will be procured

(i) whilst maintaining the privacy of other users, customers and third parties, and

(ii) without the disclosure of the traffic data of any party not part of the investigation.

(4) Subject to clause (14) of article 19 of the Constitution, proceedings under this section and section 70 shall be held in camera.

Issue of interception warrant for traffic data

72. (1) The High Court may grant an application for an interception warrant under section 71 to collect or record traffic data stored or in real-time if the Court is satisfied that

(a) the senior investigative officer authorised by a designated officer has complied with subsections (2) and (3) of section 71;

(b) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;

(c) measures shall be taken to ensure that the traffic data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and

(d) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(2) The Court shall require the service provider to keep confidential the interception warrant and execution of the warrant under this section.

(3) A service provider that contravenes subsection (2) commits an offence and is liable on summary conviction to a fine of not less than ten thousand penalty units and not more than twenty thousand penalty units.

Application for interception of content data

73. (1) A designated officer may apply ex-parte to the High Court for an interception warrant to collect or record content data.

(2) A designated officer who makes an application under subsection (1) shall demonstrate to the satisfaction of the Court that there are reasonable grounds to authorise the interception of content data and associated traffic data, related to or connected with a person or premises under investigation for one of the following purposes:

(a) in the interests of national security;

(b) the prevention or detection of a serious offence;

(c) in the interests of the economic well-being of the citizenry, so far as those interests are also relevant to the interests of national security; or

(d) to give effect to a mutual legal assistance request.

(3) Where a designated officer makes an application under subsection (1), the officer shall

(a) explain why the designated officer believes the content data sought, will be available to the person in control of the computer or computer system;

(b) identify and explain the type of content data suspected to be found on the computer or computer system;

(c) identify and explain the subscribers, users or unique identifier that may be found on a computer or computer system that is the subject of an investigation or prosecution;
(d) identify and explain the offences in respect of which the warrant is sought; and
(e) indicate what measures shall be taken to prepare and ensure that the content data will be procured
(i) whilst maintaining the privacy of other users, customers and third parties; and
(ii) without the disclosure of the data of any party not part of the investigation.

(4) Subject to clause (14) of article 19 of the Constitution, proceedings under this section and section 70 shall be held in camera.

Issue of interception warrant for content data

74. (1) The High Court may grant an application for an interception warrant under section 73 to collect or record content data stored or in real-time if the Court is satisfied that
(a) the designated officer has complied with subsections (2) and (3) of section 73;
(b) the extent of interception is commensurate, proportionate and necessary for the purposes of a specific criminal investigation or prosecution;
(c) measures shall be taken to ensure that the content data is intercepted whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; and
(d) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(2) The interception warrant issued under subsection (1) shall require a service provider, to
(a) intercept that content data stored or in real-time; and
(b) provide that content data to the officer immediately.

(3) The Court shall require the service provider to keep confidential an interception warrant issued under this section.

(4) A service provider who contravenes subsection (3) commits an offence and is liable on summary conviction to a fine of not less than ten thousand penalty units and not more than twenty thousand penalty units.

(5) Subject to this section, the Chief Justice shall designate a court or a Justice of the High Court for the purpose of considering a request for warrant made under this section.

Duration and extension of a production order or an interception warrant

75. (1) A production order or an interception warrant issued under section 70, 72 or 74 is valid for the period specified in the production order or interception warrant and may be extended.

(2) Where an extension is necessary, an investigative officer, a senior investigative officer or a designated officer, as the case may be, may apply to the High Court to obtain an extension of that production order or interception warrant.

(3) An application for an extension of a production order or an interception warrant to collect or record

(a) subscriber information,

(b) traffic data, or

(c) content data

is subject to the same conditions for the issue of the production order or interception warrant.

Interception capability

76. (1) The Authority may request a service provider to install an interception capability to enforce interception warrants issued by a court of competent jurisdiction.

(2) The Authority shall specify the requirements for the interception capability based on relevant technology and security standards.

(3) A service provider required by the Authority to install an interception capability under subsection (1) shall appoint a focal person to oversee the execution of interception warrants and related matters in the organisation concerned.

(4) A focal person appointed under subsection (3) is subject to security clearance by the National Security Co-ordinator.

(5) Equipment obtained for the purpose of the interception capability under this Act shall not be

(a) installed, managed or monitored in a foreign country; or

(b) in a form to enable the equipment to be remotely accessed from a foreign country for the purposes of maintenance.

(6) A service provider required to obtain an interception capability shall take the necessary steps to have the ability to decrypt a telecommunication message.

(7) A service provider that is required to obtain an interception capability shall bear the cost of the installation or modification of the interception capability.

(8) The requirement for the installation of an interception capability applies to a domestic service provider.

(9) A service provider which is a body corporate that contravenes subsection (5) commits an offence and is liable on summary conviction to a fine of not less than ten thousand penalty units and not more than twenty thousand penalty units.

(10) The Chief Executive Officer, Deputy Chief Executive Officer, Chief Legal Officer or the officer-in-charge of finance for the service provider that commits an offence under subsection (9) shall be deemed to have also committed the offence.

(11) A person shall not be convicted of an offence pursuant to subsection (10), where it is proved to the satisfaction of the Court that, having regard to the nature of the offence

(a) that person did not consent to, or did not connive in the commission of the offence, or

(b) that person did exercise the degree of reasonable diligence as in the circumstances ought to have been exercised to prevent the commission of the offence.

(12) A service provides who fails to comply with a request of the Authority under subsection (1) or who contravenes subsection (6) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Retention of data

77. (1) A service provider shall retain

(a) subscriber information for at least six years;

(b) traffic data for a period of twelve months; and

(c) relevant content data for a period of twelve months.

(2) Where it is necessary for traffic data and content data to be retained for more than twelve months, the investigative officer, the senior investigative officer authorised by a designated officer or the designated

officer, as the case may be, may apply ex-parte to the High Court, for an extension of the period.

(3) Where the Court grants an order for an extension, the order shall

(a) indicate the period of the extension; and

(b) be served on the service provider.

(4) A service provider or any other person who has access to data retained, processed or retrieved in accordance with this Act shall not use that data for a purpose other than what is stated in an interception warrant.

(5) A service provider or any other person who contravenes subsection (1) or (4) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Realisation of Property

Freezing of assets

78. (1) Where on an application by the Authority, the Court is satisfied that the Authority has reasonable grounds to suspect that a person has committed or is committing an offence under this Act or has been involved in a crime in cyberspace, the Court may by an order

(a) restrain that person or any other person acting on behalf of that person or a person holding assets on behalf of that person from disposing, transferring or pledging an asset or making a withdrawal from an account or deposit at a bank or financial institution;

(b) attach the assets due or owing, or belonging to, or held by or on behalf of that person;

(c) compel that person to make a full disclosure within the time specified in the order, of all assets and the nature and source of the assets;

(d) compel the person named in the order to make a full disclosure of the assets held on behalf of that person; or

(e) direct the opening, in the presence of a person authorised by the Authority, of a safe deposit box held on behalf of the person named in the order.

(2) An order under subsection (1) shall be served on the person named in the order.

(3) Where an order is made under paragraph *(a)* or *(b)* of subsection (1), the Authority may give notice of the order to all persons who may hold or be vested with property belonging to or held on behalf of the person named in the order.

(4) Where a notice is published under subsection (3), a person who allows, procures or facilitates the disposal of money or property belonging to the person named in the order, commits an offence.

(5) An order under paragraph *(a)* or *(b)* of subsection (1), shall remain in force until the final determination of the matter involving the person named in the order.

Realisation of property

79. (1) Where an order freezing assets is made under subsection (1) of section 78, and the freezing order is not discharged or not subject to an appeal, the Court shall on an application by the Attorney-General, direct

(a) the Attorney-General to manage the property;

(b) the Attorney-General to take possession of the realisable property subject to the conditions specified by the Court;

(c) a person who has possession of the realisable property to surrender possession of the property to the Attorney-General;

(d) the Attorney-General to dispose of the realisable property in a manner as directed by the Court; or

(e) a person who holds an interest in the property to make payment to the Attorney-General in respect of a beneficial interest held by the respondent or the recipient of a gift specified in this Act as the Court shall direct.

(2) The Court shall transfer, grant or extinguish the interest in the property on payment being made under paragraph *(e)* of subsection (1).

(3) The Court shall give a person who holds interest in the property reasonable opportunity to make representation to the Court before making an order under paragraph *(b)*, *(c)*, *(d)* or *(e)* of subsection (1) and also under subsection (2).

Utilisation of proceeds of realisable property

80. (1) The Court shall direct that seventy per cent of the amount realised be paid to the Authority to defray the expenses of the Authority.

(2) The Court shall direct the Attorney-General to pay ten per cent of the amount realised to the Office of the Attorney-General.

(3) The Attorney-General shall, after payment is made under subsections (1) and (2), pay the rest into the Consolidated Fund.

Industry Forum

Establishment of Industry Forum

81. (1) There is established under this Act, an Industry Forum which is a platform that periodically brings the industry together to discuss matters of common interest to the industry.

(2) The Authority may designate a body by notice within the industry to be the facilitator for the Forum if the Authority is satisfied that the body

(a) is capable of performing the function required under this section;

(b) has the administrative capacity to facilitate the Forum; and

(c) has agreed in writing to be the facilitator for the Forum.

(3) A cybersecurity service provider, service provider, telecommunications network operator and any other person concerned with matters of the industry may participate in the activities of the Forum.

(4) The Authority may decide that a body that was previously designated to be the facilitator for the Forum shall no longer be the facilitator if the Authority is satisfied that the body has ceased to meet the requirements set out in subsection (2).

(5) A designation or withdrawal of designation under this section shall take effect from the time specified by the Authority.

(6) Until the Authority designates a facilitator, the Authority shall facilitate the meetings of the Forum.

(7) The Minister and the Authority shall participate in the Forum as observers.

Industry code

82. (1) An Industry Forum may

(a) on its own initiative, or

(b) upon request by the Authority,

prepare a voluntary industry code to deal with a matter provided for in this Act.

(2) The code is not effective until the code is registered by the Authority.

(3) The Authority shall register a voluntary industry code if the code is consistent with

(a) the objects of the Authority,

(b) Regulations, standards and Guidelines made under this Act,

(c) the provisions of this Act which are relevant to the particular matter or activity.

(4) The Authority may refuse to register a code if the Authority is satisfied that sufficient opportunity for public consultation has not been given in the development of the code by the Forum.

(5) If registration of the code is refused, the Authority shall notify the Forum in writing and provide the reasons for the refusal within thirty days of the refusal.

(6) If the Authority

(a) fails to register a code within thirty days after the date that the code was submitted for registration, and

(b) does not give the Forum notice of the refusal to register the code and the reasons for the refusal within the required period the Authority shall be deemed to have registered the code.

Miscellaneous Provisions

International co-operation

83. (1) The Authority shall in the performance of the functions of the Authority, promote the security of cyberspace through international co-operation.

(2) The Authority shall implement relevant measures for the effective implementation and enforcement of international treaties on cybercrime and cybersecurity, of which Ghana is a signatory.

(3) For the purposes of international co-operation, the Authority shall designate and maintain a 24/7 contact point to tackle cybercrime.

(4) The 24/7 contact point shall provide assistance in respect of
(a) technical advice to other contact points;
(b) the expeditious preservation of data and evidence;
(c) information on the detection of suspects and related matters;
(d) the immediate transmission of legal requests in accordance with applicable laws and treaties; and
(e) any other matter related to paragraphs *(a)* to *(d)*.

Immunity of members of the Authority

84. A member of the Board and an officer of the Authority shall enjoy immunity from civil liability for actions taken or omitted to be taken in good faith in the performance of the functions of the Authority.

Cybersecurity Risk Register

85. (1) The Authority shall establish and maintain an electronic Cybersecurity Risk Register for the country.

(2) The Register shall contain details of the
(a) personal data of the owners of critical information infrastructure;
(b) identified and potential risks; and
(c) level of impact of risk.

(3) Information contained in the Register shall not be disclosed to any person other than an employee of the Authority who is responsible for keeping the Register.

(4) Despite subsection (3), the Authority may disclose information contained in the Register if required by law.

(5) Subject to article 135 of the Constitution, nothing in this enactment shall preclude the Authority from pleading in proceedings relating to information held in the custody or records of the Authority, that the production or disclosure of that information may be
(a) prejudicial to the security of the State; or
(b) injurious to the public interest.

Request for information

86. (1) The Authority may in writing direct
(a) a person who owns or operates a critical information infrastructure,

(b) a designated Sectoral Computer Emergency Response Team, or

(c) a service provider

to provide the Authority with relevant information for the purpose of ensuring the cybersecurity of the country.

(2) A person who contravenes subsection (1) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

(3) Where a contravention under subsection (1) continues, the person is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Blocking, filtering and taking down of illegal content

87. (1) The Authority may, on the order of a court, authorise a service provider to block, filter or take down illegal content and phone numbers used for a malicious purpose which seeks to undermine the cybersecurity of the country.

(2) The grounds for blocking, filtering and taking down illegal content and phone numbers include

(a) the protection of national security;

(b) the protection of children;

(c) the public safety;

(d) the prevention or investigation of a disorder or a crime;

(e) the protection of health;

(f) the protection of reputation or the rights of an individual;

(g) the prevention of the disclosure of information received in confidence;

(h) compliance with a legal order; or

(i) any other ground that the Authority may determine.

(3) A service provider who fails to comply with an authorisation made pursuant to subsection (1) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

(4) Where a contravention under subsection (1) continues, the service provider concerned is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

(5) Where a contravention under subsection (1) continues after one month, a person commits an offence and is liable on summary conviction to a fine of not less than one thousand penalty units and not

more than ten thousand penalty units or to a term of imprisonment of not less than one year and not more five years, or to both.

Co-operation

88. A public institution or a private institution shall co-operate with the Authority for the purpose of ensuring the cybersecurity of the country.

Oath of Secrecy

89. (1) The members of the Board, the Joint Cybersecurity Committee and staff of the Authority shall, before assuming office, take and subscribe to the Oath of Secrecy as set out in the Third Schedule.

(2) A person referred to under subsection (1) shall not disclose any information obtained by the Authority.

(3) Despite subsection (2), a person referred to in subsection (1), may disclose information obtained by the Authority if that information is required

(a) to enable the Authority carry out the functions of the Authority;

(b) for the prevention or detection of an offence;

(c) in compliance with the discharge of an obligation under an international agreement;

(d) to comply with a court order; or

(e) in accordance with the Right to Information Act, 2019 (Act 989).

(4) A person who contravenes subsection (2) commits an offence and is liable on summary conviction to a fine of not less than two hundred and fifty penalty units and not more than five hundred penalty units or to a term of imprisonment of not less than one year and not more than two years or to both.

Trial court and procedural powers

90. (1) The High Court shall have jurisdiction

(a) to try an offence under this Act; and

(b) in any other matter arising under this Act.

(2) The procedural powers specified under the Electronic Transactions Act, 2008 (Act 772) and any other applicable enactment shall apply under this Act.

Guidelines

91. The Authority shall publish guidelines that the Authority considers necessary for

(a) the identification of critical information infrastructure;
(b) the registration of critical information infrastructure;
(c) the protection of critical information infrastructure;
(d) the management of critical information infrastructure;
(e) access to, transfer and control of data in critical information infrastructure;
(f) the storage or archiving of data or information in critical information infrastructure;
(g) reporting incidents involving critical information infrastructure; and
(h) any other matter required for the adequate protection of critical information infrastructure.

Directives

92. (1) The Authority may issue directives to an owner of a critical information infrastructure, a cybersecurity service provider or service provider for the purpose of ensuring the cybersecurity of the country.

(2) An owner of a critical information infrastructure, a cybersecurity service provider or a service provider who fails to comply with the directives issued under subsection (1) is liable to pay to the Authority the administrative penalty specified in the Second Schedule.

Administrative penalties for contraventions

93. The Authority shall, for the purpose of imposing an administrative penalty under this Act, take into account

(a) the size of the service provider concerned;
(b) the criticality of the sector;
(c) the impact of the contravention; and
(d) any other relevant criterion determined by the Minister.

Unlawful access

94. A person who, without lawful authority retrieves subscriber information or intercepts traffic data or content data, commits an offence and is liable on summary conviction to a fine of not less than two thousand five hundred penalty units and not more than fifteen thousand penalty units or to a term of imprisonment of not less than two years and not more than five years or, to both.

General penalty

95. A person who contravenes a section of this Act for which a penalty is not provided commits an offence and is liable on summary conviction to a fine of not less than two thousand, five hundred penalty units and not more than twenty thousand penalty units or to a term of imprisonment of not less than two years and not more than five years or to both.

Regulations

96. The Minister may, by legislative instrument, make Regulations to provide for

(a) the forms for applications;
(b) authorisations and licences;
(c) the use of equipment to intercept or disable a digital technology service or product by authorised persons to execute an interception warrant;
(d) accreditation of cybersecurity professionals and practitioners;
(e) the operaionalisation of a platform for cross-sector engagement on matters of cybersecurity for effective co-ordination and cooperation between key public institutions and the private sector;
(f) the promotion and development of cybersecurity to ensure a secured and resilient digital ecosystem;
(g) certification of cybersecurity products and technology solutions;
(h) implementation of early warning system;
(i) receipt of complaints by the National Computer Emergency Response Team from Sectoral Computer Emergency Response Teams, citizens and other similar international bodies;
(j) the modalities for
  (i) the preservation of data; and
  (ii) the retention of data;
(k) dispute resolution;
(l) amendment of the administrative penalties specified in the Second Schedule; and
(m) any other matters necessary for the effective implementation of this Act.

Interpretation

97. In this Act, unless the context otherwise requires,

"Authority" means the Cybersecurity Authority established under section 2;

"Board" means the governing body of the Authority established under section 5;

"24/7 contact point" means the focal point of contact that works twenty-hours daily to facilitate or directly provide technical advice, preserve data, collect evidence, give legal information and locate suspects;

"child" means a person below the age of eighteen years;

"Committee" means the Joint Cybersecurity Committee established under section 13;

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"Computer Emergency Response Team" includes a group of experts who are tasked with operations supporting the detection, analysis and containment of a cyber incident and the response and involves qualified personnel, technology systems and processes to handle incident response operations;

"computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes

(a) an information system; and

(b) an operational technology system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system;

"content data" means the communication content of the communication, that is, the meaning or purport of the communication, or the message or information being conveyed by the communication other than traffic data;

"critical information infrastructure" means a computer or computer system designated under subsection (1) of section 35;

"cybercrime" means the use of cyberspace, information technology or electronic facilities to commit a crime;

"cybersecurity" means the state in which a computer or computer system is protected from unauthorised access or attack for the purpose of ensuring that

(a) the computer or computer system continues to be available and operational;

(b) the integrity of the computer or computer system is maintained; and

(c) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained;

"cybersecurity activity" means any activity engaged in to protect a digital system or a digital service;

"cybersecurity community" means the public and private sector stakeholders who engage in a cybersecurity activity;

"cybersecurity incident" means any act or attempt, successful or unsuccessful, to gain unauthorised access to, disrupt or misuse an information system or information stored on such information system;

"cybersecurity practitioner" means an individual or a firm that protects a computer system or digital service;

"cybersecurity products" includes

(a) a computer,

(b) a computer system,

(c) a computer programme, or

(d) a computer service

designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of another computer or computer system;

"cybersecurity professional" means a person accredited under this Act to perform a cybersecurity-related professional function;

"cybersecurity service" means the services specified in the First Schedule;

"cybersecurity service provider" means a person licensed under this Act to provide a cybersecurity service;

"Cybersecurity Risk Register" means a catalogue or database of cybersecurity threats which are published by the Authority pursuant to section 85;

"cybersecurity threat" means an unauthorised effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system;

"cyberspace" means the connected network of information technology infrastructure comprising telecom networks, the internet, computer networks, information systems, information processing and control systems and databases where people perform social acts without being limited by space and time;

"designated officer" means any of the following persons:

(a) the Director-General of the Bureau of National Investigations;

(b) the National Security Coordinator;

(c) the Inspector-General of Police;

(d) the Commissioner-General of the Ghana Revenue Authority;

(e) the Director-General, Defence Intelligence;

(f) the Executive Director, Economic and Organised Crime Office;

(g) the Director-General, Narcotics Control Commission;

(h) the Comptroller-General, Immigration Service;

(i) the Director-General, Research Department of the Ministry of Foreign Affairs;

(j) the Chief Executive Officer of the Financial Intelligence Centre; or

(k) the Attorney-General, acting upon the request of a competent authority of a foreign country;

"digital ecosystem" means the system of technical and material facilities to create, transmit, collect, process, archive and exchange information in national cyberspace comprising:

(a) transmission systems including the national transmission system, internationally connected transmission systems, satellite systems and transmission systems of enterprises providing services on telecom

networks and on the internet and other added value services in cyberspace;

(b) core service systems comprising the national information flow and navigation system, the national domain name resolution system, the national authentication system, service supply systems for internet connection and access of service providers on telecom networks, the internet and providers of other added value services in cyberspace;

(c) information technology services and applications comprising online services, and information technology applications with network connection serving management and operations by agencies, organisations and important financial and economic groups, and the national database;

(d) online services comprise e-government, e-commerce, websites, online forums, social networking and blogs; and

(e) infrastructure of smart cities, the internet of things, complex virtual reality systems, cloud computing, large data systems, fast data systems and artificial intelligence systems;

"Director-General" means the person appointed under section 15;

"e-services" means goods and services provided electronically by a service provider;

"Fund" means the Cybersecurity Fund established under section 29;

"Government e-services" means all government goods and services applied for electonically;

"interception capability" means the ability to intercept an electronic communications network, a device, a computer system, a mechanism or content data through a computer system, a device or a telecommunication facility that is capable of

(a) selectively wiretapping a telecommunication service of a subscriber; and

(b) storing information related to the communication for a specified duration;

"interception warrant" means a warrant that is issued by the High Court for the purpose of

(a) interception of a telephone or other electronic or cyberspace communication;

(b) the acquisition and disclosure of data relating to communications;

(c) the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; or

(d) the acquisition and retention of bulk personal datasets, electromagnetic emissions from a computer set and other information, traffic data and content data;

"internet service provider" means a person who provides internet service;

"investigative officer" means an officer of a law enforcement agency established by law;

"law enforcement agency" means

(a) the Police;

(b) the Customs Division of the Ghana Revenue Authority; and

(c) any other agency authorised by law to exercise the powers of the Police;

"licensee" means the holder of a licence issued by the Authority;

"Minister" means one of the Ministers specified under subsection (1) of section 5 assigned responsibility for cybersecurity matters;

"owner of critical information infrastructure" means the legal owner or operator of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner;

"phone number" includes a mobile phone and other telephone numbers for communication purpose;

"production order" means an order issued by the High Court for a computer data or subscriber information that are in the possession or control of an individual or a service provider;

"prohibited intimate image and visual recording" includes

(a) moving or still image that depicts

(i) the person engaged in an intimate sexual activity that is not ordinarily done in public; or

(ii) the genital or anal region of a person, when the genital or anal region is bare or covered only by underwear; and

(b) an image that has been altered to appear to show any of the things mentioned in paragraph *(a)* even if the thing has been digitally obscured, if the person is depicted in a sexual way;

"public key infrastructure" means the key which is available to the public for purposes of the encryption of an electronic key which is linked to a private decryption key held exclusively by the issuer of the key available to the public;

"publish" means

(a) distribute, transmit, on-demand child sexual abuse, stream, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(b) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(a)*, *(b)* or *(c)* of subsection (1) of section 62; and

(c) print, photograph, copy or make in any other manner whether of the same or of a different kind or nature to carry out an act referred to in paragraph *(a)*, *(b)* or *(c)* of subsection (1) of section 62;

"Sectoral Computer Emergency Response Team" means teams that have been established by the Authority to operate in a specific sector or institution pursuant to section 44;

"serious offence" means any offence committed within or outside the country which

(a) undermines the confidentiality, integrity and availability of computer systems and digital services;

(b) compromises the critical information infrastructure of the country;
(c) undermines the security of the country; and
(d) any other similar offence or related prohibited activity punishable with imprisonment for a period of not less than twelve months;

"service provider" includes
(a) a public or private entity that provides users of the service of the entity, the ability to communicate by means of a computer system, electronic communication devices, mobile networks; and
(b) an entity that processes or stores computer data on behalf of a communication service or a user of a communication service;
(c) an entity that provides services including data and content delivered or executed in full by a technical system involving
(i) computer time;
(ii) computer output;
(iii) data processing; and
(iv) the storage or retrieval of a programme or data through multiple platforms and devices such as web or a mobile device;

"subscriber" means a customer or a user of an electronic communications network, electronic communications service or broadcasting service;

"subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of the services of a service provider other than traffic or content data and by which may be established
(a) the type of communication service used, the technical provisions taken in respect of the communication service and the period of service;
(b) the identity, postal or geographic address, telephone and other access number of the subscriber, billing and payment information available on the basis of the service agreement or arrangement; and

(c) any other information on the site of the installation of a communication equipment, available on the basis of the service agreement or arrangement;

"telecommunication message" includes a telephone message or any other electronic or cyberspace communication message and the content and associated data of that message or communication;

"telecommunications network operator" means a person who provides a telecommunications service which includes

(a) the transmission, emission or reception of signals;
(b) writing;
(c) pulses;
(d) images;
(e) sounds; or
(f) intelligence of any kind by wire, radio, terrestrial, submarine cables, optical spectrum, electromagnetic spectrum or any other technology;

"terrorist act" means an act performed in furtherance of a political, ideological, religious, racial or ethnic cause and

(a) causes serious bodily harm to a person;
(b) causes serious damage to property;
(c) endangers the life of a person;
(d) creates a serious risk to the health or safety of the public;
(e) involves the use of firearms or explosives;
(f) releases into the environment or exposes the public to
  (i) dangerous, hazardous, radioactive or harmful substances;
  (ii) toxic chemicals; or
  (iii) microbial or other biological agents or toxins;
(g) is prejudicial to national security or public safety;
(h) is designed or intended to disrupt
  (i) a computer system or the provision of services directly related to communications;
  (ii) banking or financial services; or
  (iii) utilities or transportation; or

(i) is designed or intended to cause damage to essential infrastructure;

"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 origin, destination, route, time, date, size or duration of the communication or the type of underlying service;

"unauthorised access" means access of any kind by a person to a programme or data held in a computer without authority if

(a) the person is not personally entitled to control access of the kind in question to the programme or data; and

(b) the person does not have consent to access the kind of programme or data from the person who is entitled to control access;

"unique identifier" means a numeric or alphanumeric string that is associated with a single entity within a given computer system; and

"unwanted sexual activity" means non-consenting sexual activity;

"user" means

(a) a customer or subscriber of an electronic communications network, electronic communications service or broadcasting service; or

(b) a customer that is an operator or provider of an electronic communications network or electronic communications service.

Repeals and savings

98. (1) Sections 118 and 136 of the Electronic Transactions Act, 2008 (Act 772) are repealed.

(2) Despite the repeal of sections 118 and 136, any notices, orders, directions, appointments or instruments issued or made under the repealed provisions shall continue in force until reviewed, cancelled or terminated.

Consequential amendments

99. (1) The Electronic Transactions Act, 2008 (Act 772) is amended

(a) by the deletion of the heading "Cyber Inspectors" before section 98; and

(b) in section 144 by the deletion of the definition of "cyber inspector".

(2) The Extradition Act, 1960 (Act 22) is amended in the First Schedule by the addition of the following after "Falsification of Currency and Similar Offences":

"Cyber Offences

An offence under sections 107 to 123 of the Electronic Transactions Act, 2008 (Act 772).

Cybercrime and Cyber Offences

A cybercrime or an offence under the Cybersecurity Act, 2020 (Act .....).".

Transitional provisions

100. (1) The total sum of moneys located in any account designated for the Fund, before the coming into force of this Act shall, on the coming into force of this Act be transferred into the account of the Fund.

(2) A person who provides a cybersecurity service before the coming into force of this Act shall, within three months of the coming into force of this Act, apply to the Authority to obtain a licence.

FIRST SCHEDULE

(sections 4(k), 4(l) and 97)

Cybersecurity Services

A service provided for reward that is intended primarily for or aimed at ensuring or safeguarding the cybersecurity of a computer or computer system belonging to a person, and includes

(a) assessing, testing or evaluating the cybersecurity of a computer or computer system by searching for vulnerabilities in, and compromising the cybersecurity defences of the computer or computer system;

(b) conducting forensic examination of a computer or computer system;

(c) investigating and responding to a cybersecurity incident that has affected a computer or computer system by conducting a thorough scan and examination of the computer or computer system to identify and remove elements relating to, and identify the root cause of, the cybersecurity incident and which involves circumventing the controls implemented in the computer or computer system;

(d) conducting a thorough examination of a computer or computer system to detect any cybersecurity threat or incident that may have already penetrated the cybersecurity defences of the computer or computer system and that may have evaded detection by conventional cybersecurity solutions;

(e) designing, selling, importing, exporting, installing, maintaining, repairing or servicing of one or more cybersecurity solutions;

(f) monitoring of cybersecurity of a computer or computer system by acquiring, identifying and scanning information that is stored in, processed by, scanning information that is stored in, processed by, or transmitted through the computer or computer system;

(g) maintaining control of the cybersecurity of a computer or computer system by effecting management, operational and technical controls for the purpose of protecting the

computer or computer system against any unauthorised effort to adversely affect its cybersecurity;

(h) assessing or monitoring the compliance of an organisation with the cybersecurity policy of that organisation;

(i) providing advice in relation to cybersecurity solutions, such as

(i) providing advice on a cybersecurity programme; or

(ii) identifying and analysing cybersecurity threats and providing advice on solutions or management strategies to minimise the risk posed by cybersecurity threats;

(j) providing advice in relation to any practices that can enhance cybersecurity; or

(k) providing training or instruction in relation to any cybersecurity service, including the assessment of the training, instruction or competencies of another person in relation to any such activity.

SECOND SCHEDULE

(sections 36(4), 39(2)(a), 39(2)(b), 39(2)(c),44(6), 47(6), 49(2), 51(5), 59(4), 76 (12), 77(5), 86(2), 86(3), 87(3), 87(4), 92(2) and 96(l))

Table of Administrative Penalties

A person who fails to comply with a requirement specified in the second column of the table is liable to the administrative penalty corresponding to the requirement as specified in the third column of the table.

Column 1	Column 2	Column 3
Sections of Act creating contravention	**Contravention**	**Administrative Penalty**
36(4)	Owner of a registered critical information infrastructure failing to inform the Authority within seven days of the change in legal ownership of the registered critical information infrastructure.	Not less than five hundred penalty units and not more than ten thousand penalty units.
39(2)(a)	Owner of a critical information infrastructure failing to report a cybersecurity incident.	Not less than two hundred and fifty penalty units and not more than ten thousand penalty units.
39(2)(b)	Owner of a critical information infrastructure failing to cause an audit to be performed on the critical information infrastructure.	Not less than two hundred and fifty penalty units and not more than ten thousand penalty units.
39(2)(c)	Owner of a critical information infrastructure failing to submit a copy of the audit report to the Authority.	Not less than two hundred and fifty penalty units and not more than ten thousand penalty units.
44(6)	A Sectoral Computer Emergency Response Team failing to comply with the regulatory directives of the Authority.	Not less than five hundred penalty units and not more than five thousand penalty units.

47(6)	The head of an institution failing to report a cybersecurity incident to the relevant Sectoral Computer Emergency Response Team or the National Computer Response Team.	Not less than two hundred and fifty penalty units and not more than five thousand penalty units.
49(2)	Person providing a cybersecurity service without a licence.	Penalty equivalent to the cost of damage caused and value of the financial gain made.
51(5)	A licensed service provider using a licence for a purpose other than the purpose for which the licence was granted.	Fifty thousand penalty units.
59(4)	Person failing to comply with the cybersecurity standards.	Not less than two hundred and fifty penalty units and not more than twenty-five thousand penalty units.
76(12)	Service provider who *(a)* fails to install an interception capability to enforce an interception warrant issued by a court of competent jurisdiction; or *(b)* fails to take the necessary steps to decrypt a telecommunication message pursuant to an inter ception warrant.	Ten thousand penalty units.
77(5)	(a) Service provider who fails to retain (i) subscriber information for at least six years; (ii) traffic data for a period of twelve months; and (iii) relevant content data for a period of twelve months. (b) Person using data retained for a purpose other than what is stated in an interception warrant.	Not less than one thousand penalty units and not more than ten thousand penalty units. Not less than one thousand, five hundred penalty units and not more than ten thousand penalty units.

86(2)	The owner or operator of a critical information infrastructure, a designated Sectoral Computer Emergency Response Team or a provider of a digital service failing to submit relevant information to the Authority for the purpose of ensuring the cybersecurity of the country.	Not less than two hundred and fifty penalty units and not more than ten thousand penalty units.
86(3)	Daily default on the part of the owner of a critical information infrastructure, a designated Sectoral Computer Emergency Response Team or provider of a digital service to comply with a request to provide relevant information for the purpose of ensuring the cybersecurity of the country.	One hundred penalty units for each day that the contravention continues.
87(3)	Service provider failing to comply with an authorisation to block, filter or take down any content which seeks to undermine the cybersecurity of the country.	Not less than one thousand penalty units and not more than twenty-five thousand penalty units.
87(4)	Service provider failing on a daily basis, to comply with an authorisation to block, filter or take down any content which seeks to undermine the cybersecurity of the country.	One hundred penalty units for each day the contravention continues.
92(2)	Owner of a critical information infrastructure, a cybersecurity service provider or a provider of a digital service failing to comply with a directive issued by the Authority.	Not less than two hundred and fifty penalty units and not more than ten thousand penalty units.

THIRD SCHEDULE

Oath of Secrecy

(section 89 (1))

I .....holding the office of..... do, (in the name of the Almighty God, swear) (solemnly affirm) that I will not directly or indirectly communicate or reveal to any person any matter which shall be brought under my consideration or shall come to my knowledge in the discharge of my official duties except as may be required for the discharge of my official duties or as may be specifically provided by law.

Date of *Gazette* notification: 29th December, 2020.

PRINTED BY GHANA PUBLISHING COMPANY LTD. ASSEMBLY PRESS, ACCRA. GPCL/A063/1,250/01/2021
Website:www.ghanapublishing.com Email:info@ghanapublishing.com Tel: +233 302-664338/9