LD-O 14/2019

AN ACT TO PROVIDE FOR THE ESTABLISHMENT OF THE CYBER SECURITY REGULATORY AUTHORITY OF SRI LANKA WHICH IS THE APEX INSTITUTION RESPONSIBLE FOR ALL MATTERS RELATING TO CIVILIAN ASPECTS OF CYBER SECURITY; TO PROVIDE FOR THE IMPLEMENTATION OF NATIONAL INFORMATION AND CYBER SECURITY STRATEGIES AND POLICIES; TO PROVIDE FOR THE PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE IN ORDER TO ADDRESS THE CYBER SECURITY THREATS CHALLENGING SRI LANKA, AND TO PROVIDE FOR MATTERS CONNECTED THEREWITH OR INCIDENTAL THERETO

Be it enacted by the Parliament of the Democratic Socialist Republic of Sri Lanka as follows: -

Short title and date of operation

1. (1) This Act may be cited as the Cyber Security Act, No. of 2023.

(2) The provisions of Part VII of this Act shall come into operation on such date as the Minister may appoint by Order published in the *Gazette.*

(3) The provisions except the provisions of Part VII of this Act shall come into operation on the date on which the Bill becomes an Act of Parliament.

PART 1

OBJECTS OF THE ACT

Objects of the Act

2. The Objects of the Act shall be -

(a) to establish the Cyber Security Regulatory Authority of Sri Lanka as the apex institution responsible for all matters relating to civilian aspects of cyber security;

(b) to ensure the effective implementation of the national information and cyber security strategies, and cyber security policies as approved by the Cabinet of Ministers;

(c) to prevent, detect, mitigate and respond to cyber security threats and incidents effectively and efficiently;

(d) to provide for creation of a safe and secure cyber security environment; and

(e) to ensure effective coordination and collaboration with the Defence Cyber Command of Sri Lanka established under the Defence Cyber Command Act, No. of 2023 (hereinafter referred to as the "Command") to deal with matters on cyber security in relation to the national security.

Establishment of the Cyber Security Regulatory Authority of Sri Lanka

3. (1) (a) There shall be established an authority which shall be called the Cyber Security Regulatory Authority of Sri Lanka (hereinafter referred to as ''the Authority'') for the purposes of this Act.

(b) The Authority shall be the apex executive body for the implementation of all matters relating to civilian aspects of cyber security in Sri Lanka.

(2) The Authority shall, by the name assigned to it by subsection (1), be a body corporate having perpetual succession and a common seal and may sue and be sued in its corporate name.

Powers, duties and functions of the Authority

4. (1) The powers, duties and functions of the Authority shall be to-

(a) function as the national point of contact for civilian cyber security and to ensure national cyber security readiness;

(b) conduct security assessments for the national defence infrastructure where required by the Defence Cyber Command established under the Defence Cyber Command Act, No. of 2023.

(c) formulate and implement national cyber security strategies, policies, standards, guidelines, action plans and projects in government and in other relevant sectors, and provide necessary advice, instructions and guidance to create a resilient and trusted national cyber security ecosystem to realize the benefits of digital technologies and to facilitate its growth;

(d) assess the progress of implementation of national cyber security strategies, policies, standards, guidelines, action plans and projects by government institutions, and in other relevant sectors and make recommendations to improve cyber security resilience;

(e) perform the cyber incident response functions which were assigned to Sri Lanka Computer Emergency Readiness Team, prior to coming into operation of this Act;

(f) identify and designate, Critical National Information Infrastructure in terms of section 19, both in government and other relevant sectors, and obtain information from such Critical National Information Infrastructure on incidents relating to the civilian aspects of cyber security;

(g) establish or designate institutions, units, sectoral Computer Incidents Readiness Teams (hereinafter referred to as the "sectoral CERTs") and Computer Security Incident Response Teams (hereinafter referred to as the "CSIRTs") or any other entity to assist the Authority in the performance and discharge of the duties and functions of the Authority, in consultation with the relevant Ministries;

(h) protect Critical National Information Infrastructure and other computer systems of Sri Lanka by leading and coordinating at national level by preventing and responding to cyber threats and incidents in respect of matters relating to civilian aspects of cyber security;

(i) issue cyber security standards, guidelines and other instructions to improve and ensure the cyber resiliency of Critical National Information Infrastructure, government institutions, and other stakeholders, in consultation with relevant Regulatory Authorities where applicable;

(j) monitor the designated CNIIs owned by government and other relevant sectors through the National Cyber Security Operation Centre in order to detect, investigate and respond to potential cyber threats and incidents in respect of matters relating to the civilian aspects of cyber security;

(k) obtain information from law enforcement authorities, the Cyber Security Command, Internet Service Providers, Lanka Domain Registry, other relevant sectoral Computer Incidents Readiness Teams, Computer Security Incident Response Teams, and any other Cyber Security Service Provider on cyber threat indicator, defensive measures, cyber security risks, incidents and analysis, in relation to cyber security threats and incidents relating to the civilian aspects of cyber security;

(l) in keeping with best practices, issue instructions to Internet Service Providers in removal of harmful computer programs such as malicious bots or any other type of malware from client computers of the subscribers of Internet Service Providers, and monitoring remediation measures implemented by Internet Service Providers to prevent cyber security threats and incidents created by such activities;

(m) request reports from Critical National Information Infrastructures, government institutions, and other relevant sectors on information relating to the compliance with the cyber security strategies, policies, standards, guidelines or with any other instructions issued by the Authority;

(n) conduct cyber security assessments and audits on Critical National Information Infrastructures, government and other relevant institutions;

(o) collaborate with international agencies, authorities and foreign states in order to obtain training on cyber

security and related matters for relevant officers and authorities in Sri Lanka;

(p) conduct and manage cyber security services for government institutions and other relevant sectors on request, and where necessary, impose charges and levies as shall be prescribed by regulations for any service rendered by the Authority;

(q) with the approval of the Cabinet of Ministers, enter into agreements with or engage in any activity, either alone or in conjunction with local or international organizations for the purposes of this Act;

(r) with the approval of the Cabinet of Ministers, represent Sri Lanka internationally in matters relating to cyber security in accordance with the government procedures;

(s) facilitate the domestic implementation of international legal obligations to which Sri Lanka is a party, in order to ensure the effective implementation of cyber security strategies and cyber security policies;

(t) assist public and private organizations in developing curricula in relation to cyber security, gathering and disseminating knowledge on cyber security, providing training and education in relation to cyber security, and take necessary actions to ensure the availability of competent and highly skilled professionals in cyber security domain;

(u) promote the awareness among citizens and in relevant sectors regarding the risks in cyber space, and to engage in capacity building to protect the identity, privacy, and economic assets in cyber space;

(v) accredit individuals and firms which provide cyber security services;

(w) coordinate the conduct of sectoral cyber security drills, from time to time, to improve overall cyber security readiness;

(x) operate the Certification Authority designated under the Electronic Transactions Act, No.19 of 2006 and facilitate the implementation and promotional activities of the Electronic Transactions Act, No.19 of 2006 in consultation with the Minister of the Ministry to whom the implementation of the provisions of the said Act is assigned;

(y) acquire by way of purchase or otherwise, any movable or immovable property and hold, take or give on lease or hire, mortgage, pledge and sell or otherwise dispose of such property as may be determined by the Authority for the purpose of this Act;

(z) open and maintain bank accounts with any bank as may be determined by the Authority;

(aa) charge fees for performing powers and functions of the Authority, receive grants or contributions from any legal source and to raise funds by all lawful means and apply such funds in the exercise, performance and discharge of the power, duties and functions of the Authority:

Provided however, the Authority shall obtain prior written approval of the Ministry of Finance in respect of all foreign grants, gifts or donations;

(ab) make rules and issue directives in respect of the matters for which rules and directives are required to be issued under the provisions of this Act;

(ac) issue directions to the Director General appointed under section 14 in respect of administration and control of the affairs of the Authority; and

(ad) do all such other acts which are not inconsistent with the provisions of this Act or any other written law as may be expedient for the accomplishment of the objects of the Authority

(2) The Authority shall, for the purpose of giving effect to the provisions of this Act, designate, in consultation with the owner of any Critical National Information Infrastructure, an officer of such Critical National Information Infrastructure as an Information Security Officer in accordance with such criteria as shall be prescribed.

(3) Every Information Security Officer designated under subsection (2) shall ensure the compliance with the rules and directives issued by the Authority, from time to time, in respect of matters relating to the civilian aspects of cyber security.

Powers, duties and functions of the Authority to be exercised, discharged and performed by a Board of Directors

6. (1) The powers, duties and functions of Authority shall be exercised, discharged and performed by a Board of Directors (hereinafter referred to as the "Board") consisting of –

(a) the following ex-officio members, namely: -

(i) the Secretary to the Ministry of the Minister to whom the subject of information and cyber security is assigned or an Additional Secretary of such Ministry nominated by the Secretary of such Ministry;

(ii) the Secretary to the Treasury;

(iii) the Director General of the Defence Cyber Command, established under the Defence Cyber Command Act, No. of 2023;

(iv) the Director General of Telecommunication Regulatory Commission, established under section 22B of the Sri Lanka Telecommunications Act, No25 of 1991;

(v) Chairperson of Information and Communication Technology Agency of Sri Lanka registered under the Companies Act, No.7 of 2007; and

(b) four persons appointed by the President, (hereinafter referred to as the "appointed members") each of whom shall have over fifteen years of experience and demonstrated professional excellence in the fields of cyber security, information and communication technology, public or corporate sector administration, management, law or finance.

Chairperson of the Board

7. (1) (a) The President shall appoint from among the appointed members, a member of the Board who has demonstrated effective leadership qualities in public or private sector entities to be the Chairperson of the Board.

(b) The Chairperson shall hold office for the period of his membership of the Board.

(2) The President may for reasons assigned therefor, remove the Chairperson from the office of Chairperson.

(3) The Chairperson may resign from his office by letter addressed to the President and such resignation shall be effective from the date on which it is accepted by the President.

(4) Where the Chairperson is temporarily unable to exercise, perform and discharge the powers, duties and functions of his office due to ill health, other infirmity, absence from Sri Lanka or any other cause, the President may appoint any other appointed member to exercise, perform and discharge the powers, duties and functions of the Chairperson in addition to his normal duties as a member of the Board.

Term of office of the appointed members

8. (1) Every appointed member shall, unless he vacates office earlier, by death, resignation or removal, hold office for a period of three years from the date of his appointment.

(2) Any appointed member of the Board who vacates office shall, unless he has been removed from office under subsection (4), be eligible for re-appointment for not more than one further term of office, whether consecutive or otherwise.

(3) Any appointed member of the Commission may at any time, resign his office by letter in that behalf addressed to the Minister and such

resignation shall take effect from the date on which the resignation is accepted in writing by the Minister.

(4) The President may, for reasons assigned therefor remove any appointed member from office and who has been so removed from office shall not be eligible for re-appointment as a member of the Board or to serve the Board in any other capacity.

(5) In the event of the vacation of office by death, resignation or removal of any appointed member, the President shall, subject to paragraph (b) of subsection (1) of section 6, appoint another person to fill such vacancy and such person shall hold office for the un-expired period of the term of office of the member whom he succeeds.

(6) Where any appointed member of the Board is temporarily unable to perform the duties of his office on account of ill health or any other cause or if he is absent from Sri Lanka for a period of not less than six months, the Minister shall, having regard to the provisions of paragraph (b) of subsection (1) of section 6, appoint any other person to act in place of such member during his absence.

(7) Where any appointed member of the Board fails to attend three consecutive meetings of the Board without obtaining prior approval from the Chairperson for absence, such member shall be deemed to have vacated his office at the conclusion of the third meeting and the Minister shall appoint another person to fill such vacancy in the manner provided for in subsection (5).

Disqualification to become a member of the Board

9. (1) Any person shall be disqualified from being appointed or continue to be a member of the Board, if such person –

(a) is or becomes a Member of Parliament, Member of Provincial Council or a Member of Local Authority;

(b) is or becomes directly or indirectly, by himself or by any other person on his behalf, holds or enjoys any right or benefit under any contract made by or on behalf of the Authority, unless it has been declared by such person as specified in section 10;

(c) is under any law in force in Sri Lanka found or declared to be of unsound mind;

(d) is a person who has been declared an insolvent or bankrupt under any written law in Sri Lanka or in any other country, is discharged insolvent or bankrupt; or

(e) has been convicted of any criminal offence by any court in Sri Lanka or in any other country.

Members to disclose interest

10. (1) A member who is directly or indirectly interested in any matter dealt with by the Board or any decision that is to be taken by the Board on any such matter shall disclose the nature of such interest at the meeting of the Board where such decision is being taken.

(2) Such disclosure shall be recorded in the minutes of such meeting and such member shall not take part in any deliberation or decision of the Board with regard to that matter, and shall not participate in such meeting while such deliberations is in progress or such decision is being made.

Meetings of the Board

11. (1) The Director-General of the Board appointed under section 15 shall summon all the meetings of the Board.

(2) The Chairperson shall preside at every meeting of the Board and in the absence of the Chairperson from any meeting of the Board, any appointed member elected by the members present shall preside at such meeting.

(3) The quorum for any meeting of the Board shall be five members including the Chairperson if he is present at such meeting.

(4) A meeting of the Board may be held either –

(a) by the number of members who constitute a *quorum* being assembled at the place, date and time appointed for such meeting; or

(b) by means of audio-visual communication by which all members participating and constituting a quorum can simultaneously see and hear each participating member for the duration of the meeting.

(5) All questions for decision at any meeting of the Board shall be decided by vote of the majority of members present and voting at such meeting. In the case of an equality of votes, the Chairperson or the member presiding in the absence of the Chairperson shall, in addition to his vote, have a casting vote.

(6) The meetings of the Board shall be conducted in conformity with the rules made and procedure established by the Board in that behalf, from time to time.

Remuneration of members

12. The members of the Authority other than *ex-officio* members, may be remunerated in such manner in consultation with the Minister assigned the subject of Finance and shall carry out their functions subject to such terms and conditions as may from time to time be determined by the President.

Seal of the Authority

13. (1) The seal of the Authority -

(a) shall be in the custody of a member of the Board as may be determined by the Board, from time to time;

(b) may be altered in such manner as may be determined by the Board; and

(c) shall not be affixed to any instrument or document except with the sanction of the Board and in the presence of two members of the Board who shall sign the instrument or document in token of their presence and such signing shall be independent of the signing of any person as a witness.

(2) The Board shall maintain a register of the instruments and documents to which the seal of the Authority has been affixed.

Act, decision or proceeding of the Board not to be invalid

14. Any act, decision or proceeding of the Board shall not be invalid by reason only of the existence of any vacancy in the Board or any defect in the appointment of a member of the Board.

PART II

APPOINTMENT OF THE DIRECTOR-GENERAL AND THE STAFF OF THE AUTHORITY

Director-General of the Authority

15. (1) The Board shall appoint a Director General of the Authority who have achieved eminence, integrity and has proven professional expertise in providing leadership to public sector or private sector, and who shall not be a member of any political party.

(2) The Director-General shall be the chief executive officer of the Authority and the conditions of employment including remuneration of the Director-General shall be determined by the Board in accordance with the rules made by the Authority.

(3) The Board shall not appoint any person as the Director General of the Authority, if such person –

(a) has been previously found guilty of serious misconduct by a court or tribunal or has been subject to a disciplinary action by a regulatory body;

(b) has been previously dismissed from office; or

(c) has committed a breach of the provisions of this Act, or regulations, rules or directives made thereunder.

(4) The Director General shall, subject to the general directions and control of the Board –

(a) be charged with the administration and control of the affairs and transactions of the Authority including the administration and control of the staff;

(b) be responsible for the execution of all decisions of the Board;

(c) exercise such powers, duties and functions of the Authority under this Act as may be assigned to him by the Board.

(5) The Director General shall hold office for a period of three years from the date of appointment and shall be eligible for reappointment.

(6) Whenever the office of the Director General becomes vacant upon the death, removal from office or resignation by letter in that behalf addressed to the Board, the Board may, having regard to the provisions of subsection (1) appoint any other senior officer of the staff of the Authority to perform the functions of the Director General until another person is appointed to fill such vacancy.

(7) The Director General shall attend the meetings of the Board but shall not have the right to vote at any such meeting.

(8) The Director General may be removed from office by the Board with the approval of the Minster in the event that -

(a) there is a likelihood of any conflict of interests in carrying out by the Director-General, the duties and functions assigned to him under this Act;

(b) the Director-General becomes permanently incapacitated and incapable of performing his duties;

(c) the Director-General has done any act which is of a fraudulent or illegal character or is prejudicial to the interest of the Authority; or

(d) the Director-General has failed to comply with any rule made under this Act or directives issued by the Authority.

(9) The Director General may with the approval of the Board, delegate to an officer of the staff of the Authority, in writing any power or function assigned to him by this Act and such officer shall exercise and discharge such power or function subject to the direction and control of the Director General.

Officers and employees of the Authority

16. (1) Notwithstanding anything to the contrary in any other written law, the Authority may create cadre positions and employ officers and employees as it considers necessary for the efficient discharge of its functions and may fix their salaries and wages or other remuneration,

benefits and pensions of such officers and employees for the purposes of carrying out its duties and functions under the provisions of this Act.

(2) The Authority shall promote and sponsor the training of technical personnel on the subjects of information technology and cyber security, privacy and personal data protection, analytics, information technology, law and other related subjects and for this purpose, the Authority shall be authorised to defray the costs of study, in Sri Lanka or abroad of the officers and employees of the Authority who are of proven merit as determined by the Authority.

(3) The officers and employees of the Authority shall be subject to the provisions of a code of conduct which shall be applicable to them, prepared and revised, from time to time, by the Authority in accordance with the rules of the Authority.

(4) The Authority shall not appoint any person to the staff of the Authority where such person–

(a) has been previously found guilty of serious misconduct by a court or tribunal or has been subject to a disciplinary action by a regulatory body;

(b) has been previously dismissed from office; or

(c) has acted in contravention of the provisions of this Act or any regulation or rule made thereunder or any directives issues thereunder.

Appointment of public officers to the staff of the Authority

17. (1) At the request of the Authority any officer in the public service may, with the consent of the officer and the Public Service Commission established by the Constitution be temporarily appointed to the Authority for such period as may be determined by the Authority or with like consent, be permanently appointed to such staff.

(2) Where any officer in the public service is temporarily appointed to the staff of the Authority, the provisions of subsection (2) of section 14 of the National Transport Commission Act, No. 37 of 1991, shall *mutatis mutandis*, apply to and in relation to such officer.

(3) Where any officer in the public service is permanently appointed to the staff of the Authority, the provisions of subsection (3) of section 14 of the National Transport Commission Act, No. 37 of 1991, shall mutatis mutandis, apply to and in relation to such officer.

(4) Where the Authority employs any person who has agreed to serve the Government for a specified period, any period of service to the Authority by that person shall be regarded as service to the Government for the purpose of discharging the obligations of such agreement.

(5) The Authority may with the consent of such officer or employee propose secondment of its officers or employees to other state institutions or regulatory authorities in Sri Lanka or abroad for a period determined by the Board on an assignment agreed upon between such institution and the Authority. The period of secondment shall be deemed to be considered as service to the Authority.

Winding up of the CERT Private (Ltd)

18. (1) The Sri Lanka Computer Emergency Readiness Team Private (Ltd) (in this Act referred to as the "CERT Private (Ltd)") which is incorporated as a company under Companies Act, No.07 of 2007, shall be wound up with effect from the date on which the Bill becomes an Act of Parliament.

(2) Upon winding up the CERT Private (Ltd) –

(a) it shall become part of the Authority primarily focusing on Incidents Response and shall be renamed as Sri Lanka Computer Emergency Response Team.

(b) all property movable and immovable belonging to the CERT Private (Ltd), together with all its assets and liabilities shall with effect from the date of the coming into operation of this Act, be transferred to the Authority; and

(b) the powers and functions exercised by the CERT Private (Ltd) immediately before the date on which the Bill becomes an Act of Parliament shall continue to be exercised by the Authority.

(3) The provisions relating to winding up of Companies specified in the Companies Act, No.07 of 2007 shall *mutatis mutandis* apply in respect of the winding up of the CERT Private (Ltd), under this section.

Officers and employees of the staff of the CERT Private (Ltd)

19. (1) Notwithstanding the winding up of the CERT Private (Ltd) in terms of section 17, the officers and employees of the CERT Private (Ltd) who on the day immediately preceding the date on which the Bill becomes an Act of Parliament be offered employment in the Authority on such terms and conditions as may be agreed upon the Authority and such officers and employees.

(2) When an officer or employee referred to in subsection (1), who wishes to opt out of serving in the Authority, may do so within three months from the date on which such officer or employee was notified of the option by the Authority.

(3) All officers and employees who are offered employment in the Authority and who have expressed the desire to accept employment in the Authority shall become employees of the staff of the Authority with effect from the date of acceptance of employment.

(4) The officers and employees who have become employees of the Authority shall be employed on terms not less favourable than their terms of employment in the CERT Private (Ltd), and the period of service rendered by them to the CERT Private (Ltd) shall be regarded as a service rendered to the Authority.

(5) Where any officer or employee of the CERT Private (Ltd) expresses his desire not to accept employment in the Authority shall be deemed to have retired from service form the date on which such officer or employee was notified of the option by the Authority, and shall be eligible for the retirement benefits that such officer or employee would have been entitled to, if he retired from service in the CERT Private (Ltd) after reaching his age of retirement.

PART III

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Designation of a computer system &c. as Critical National Information Infrastructure

20. (1) The Authority shall, in consultation with relevant authorities, identify any computer, computer program, computer system or any related device located wholly or partly in Sri Lanka, as a Critical National Information Infrastructure.

(2) The Authority shall, when any computer, computer program, computer system or any related device is identified as a Critical National Information Infrastructure, inform such fact to the owner computer, computer program, computer system or any related device and the relevant regulatory authority which regulates or supervises such Critical National Information Infrastructure of such owner.

(3) The Authority may if it considers appropriate, obtain the views of the owner of such Critical National Information Infrastructure relating to such a Critical National Information Infrastructure and publish such Critical National Information Infrastructure in the *Gazette*.

Responsibility of an owner of a CNII

21. (1) Upon the identification of a Critical National Information Infrastructure, the owner of such Critical National Information Infrastructure shall -

(a) (i) be responsible for ensuring cyber security of such Critical National Information Infrastructure, in conformity with the prescribed requirements;

(ii) if such Critical National Information Infrastructure spreads across multiple institutions or multiple sectors, every owner of such institution or sector shall become jointly and severally responsible for the protection of such Critical National Information Infrastructure;

(b) be responsible –

(i) for developing and implementing a protection plan for securing such Critical National Information Infrastructure against cyber security threats or cyber security incidents;

(ii) for assisting the Authority or any other institution, unit or entity established or designated by the

Authority to perform the duties and functions of the Authority under this Act;

(iii) for adopting policies, standards, and guidelines as may be prescribed for securing such Critical National Information Infrastructure;

(c) conduct security risk assessments, audits and vulnerability assessments of such Critical National Information Infrastructure, in compliance with the procedures and timelines specified by rules made by the Authority;

(d) as part of a security review, furnish information on the design, security configurations and other technical details or information relating to the operations of such Critical National Information Infrastructure or any other computer, computer program, computer system or related device under the control of such owner, to the Authority in the form, manner and within the period of time specified in accordance with the rules made by the Authority;

(e) furnish any other information which may be required to ascertain the cyber security readiness by Critical National Information Infrastructure, and the level of compliance of Critical National Information Infrastructure according to the policies, standards and guidelines issued by the Authority in the form, manner and within the period of time as specified by rules made by the Authority; and

(f) notify the Authority of the occurrence of any cyber security incident in respect of such designated Critical National Information Infrastructure or any other computer, computer program, computer system or related device under the control of the owner, in the form, manner and within a period of time as specified by rules made by the Authority.

(2) the Authority shall maintain the confidentiality of the information supplied by the owner of Critical National Information Infrastructure.

PART IV

ADVISORY COMMITTEE ON CYBER SECURITY

Advisory Committee on Cyber Security

22. (1) There shall be a committee called the Advisory Committee on Cyber Security (hereinafter referred to as the "Advisory Committee").

(2) The function of the Advisory Committee is to review evolving cyber security risks and associated technology and make recommendations to the Board.

(3) (a) The Advisory Committee shall consist of five members including the Chairperson, having eminence and proven professional expertise in the fields of cyber security, information and communication technology, and law, one of whom shall be a person representing the public sector.

(b) The Minister shall appoint one of the members of the Advisory Committee as the Chairperson.

(4) The Director General of the Authority shall be the secretary to the Advisory Committee.

(5) Without prejudice to the generality of the provisions of subsection (2), in the exercise, performance and discharge of its powers, functions and duties, the Advisory Committee shall consider the following matters referred to it by the Authority:-

(a) evolving cyber security risks and associated technologies;

(b) criteria in respect of accreditation of cyber security service providers;

(c) criteria in respect of classifying Critical National Information Infrastructure; and

(d) legal matters on cyber security and cybercrime;

(e) any other technical matters as may be requested by the Authority to be considered.

(6) The Advisory Committee shall, within the period specified in the referral referred to in subsection (4), make recommendations to the Authority on any matter referred to it by the Authority.

PART V

ACCREDITATION OF CYBER SECURITY SERVICE PROVIDERS

Cyber security service providers

23. (1) Any person or body of persons shall not engage in the business of providing the following cyber security services unless such person or body of persons has been accredited by the Authority:-

(a) to operate sectoral CERTs and CSIRTs;

(b) to conduct vulnerability assessments and penetration tests;

(c) to conduct cyber security audits and risk assessments;

(d) to monitor the cyber security through operating Cyber Security Operation Centre;

(e) to conduct cyber security forensic investigations;

(f) to provide cyber security advisory and consultative services;

(g) to design, develop, implement, install, and troubleshooting cyber security solutions;

(h) Importing, distributing, installing and maintaining cyber security solutions that safeguard computer, computer programs, computer systems, relevant devices from cyber threats and incidents; and

(i) Managing the cyber security of client organizations.

(2) Any person or body of persons who engages in cyber security service specified in subsection (1) without having a valid accreditation commits an offense and liable to an administrative penalty imposed under section 24.

(3) The procedures and conditions to grant and renewal of accreditation, the validity of accreditation, revocation or suspension of accreditation, and for any determining the cyber security services for which an accreditation shall be obtained shall be as prescribed.

PART VI

FUND OF THE AUTHORITY

Fund of the Authority

24. (1) The Authority shall have its own fund (hereinafter referred to as the "Fund").

(2) There shall be paid into the Fund –

(a) all such sums of money as may be voted, from time to time, by Parliament for the use of the Authority;

(b) all such sums of money as may be received by the Authority in the exercise, performance and discharge of its powers, duties and functions under this Act; and

(c) all such sums of money as may be received by the Authority by way of gifts, grants or donations from any local or foreign source:

Provided however, the Board shall obtain the prior written approval of the Ministry of Finance in respect of all foreign gifts, grants and donations made to the Authority.

(3) There shall be paid out of the Fund all such sums as are required to defray the expenditure incurred by the Authority in the exercise, performance and discharge of its powers, duties and functions under this Act or under any other written law and all such sums as are required to be paid out of the Fund.

PART VII

IMPOSITION OF PENALTIES

Imposition of penalties

25. (1) A person who is required to conform to the requirements of section 21 or 23 this Act, if fails to so conform, shall in the first instance be issued with a warning in writing by the Board, and given a specified period of time as may be specified in such warning to conform to such requirements, or to show cause as to why such requirements are not being complied with.

(2) Where a person fails to conform to the written warning issued under subsection (1), the Authority shall, taking into consideration the nature and gravity of such non-compliance, by notice require such person to pay a penalty not exceeding rupees one million.

(3) Where any person fails to conform to any requirement specified in section 21 or 23 in any second or subsequent occasion, such person shall in addition to the penalty imposed under this section be liable to the payment of an additional penalty of twice the amount imposed as a penalty on a precious occasion.

(4) The Authority shall be responsible for the collection of a penalty imposed under this section and the money so collected shall be credited to the Consolidated Fund.

(5) If a person who becomes liable to a penalty in terms of subsection (2) fails to pay such penalty, the Authority may make an ex-parte application to the Magistrate Court of Colombo for an order requiring the payment of the penalty recovered in alike manner as a fine imposed by such court.

(6) The imposition of a penalty under this section shall not preclude a supervisory authority or a regulatory authority from taking any other regulatory measures including, but not limited to, the suspension of any person from the carrying on of a business or profession or the cancellation of a license or authority granted for the carrying on of a business or profession, as may be permitted in terms of any applicable written law for the regulation or supervision of the relevant business or profession.

(7) Where a penalty is imposed under this section on a body of persons, then -

(a) if that body of person is a body corporate, every person who at the time of the imposition of the requirements under subsection (1) was a director, and other officer responsible with management and control of that body corporate;

(b) if that body of persons is a firm, every partner of that firm; or

(c) if that body is not a body corporate, every person who at the time of the imposition of such requirements under subsection (1) was the officer responsible with management and control of that of that body,

Shall be liable to pay such penalty unless he proves that he had no knowledge of the failure to comply with the requirement or that he exercised all due diligence to ensure compliance therewith.

(8) Without prejudice to the provisions of subsection (1) and (2), the Authority may issue a directive to any institution that has without reasonable cause failed to comply in whole or in part with any obligations specified in Parts VI of this Act.

(9) Where an Institution fails to comply with a directive issued under subsection (8), the Authority may, upon application to the High Court of the Western Province, holden in Colombo and upon satisfying the Court that such institution has failed without reasonable excuse to comply in whole or in part with the directive issued by it under subsection (7), obtain an order against such institution and any or all of the officers or employees of that institution in such terms as the Court deems necessary to enforce compliance with such directive.

Appeals

26. (1) A person who is aggrieved by the imposition of a penalty under section 24, may appeal against such decision to the Court of Appeal within twenty-one working days from the date of the notice of the imposition of such penalty was communicated to such person.

(2) Any person who prefer an application to the Court of Appeal under subsection (1), shall deposit in cash as security such sum of money equal to the penalty imposed under section 24, before the Registrar of the Court of Appeal.

(3) Where an appeal is preferred under subsection (1), the burden of proof shall be on such person, to prove that he has acted in compliance with the provisions of this Act.

Financial year and audit of accounts

27. (1) The financial year of the Authority shall be the calendar year.

(2) The provisions of Article 154 of the Constitution relating to the audit of the accounts of public corporations shall apply to the audit of accounts of the Authority.

PART VIII

MISCELLENEOUS

Power of entry, inspection and search

28. (1) Any officer of the Authority specifically authorized in writing in that behalf by the Director General may where the Director-General considers it necessary for the purpose of discharging the functions of the Authority, and for the purpose of ascertaining whether the provisions of this Act or any regulation made thereunder are being complied with, -

(a) enter, inspect and search premises of any designated CNII;

(b) conduct cyber security audits, forensic investigations or any type of cyber security assessment pertaining to such CNII;

(c) examine and take copies of any document, record or part thereof pertaining to such CNII;

(d) question any person whom the Authority has reasonable cause to believe that such person is an owner or employee of such CNII.

(2) For the purpose of carrying out any function under subsection (1), written consent to enter such premises shall be obtained from the owner, occupier or the person in charge of such premises.

(3) Where the consent required to be obtained under subsection (2) is unfairly refused, any officer of the Authority specifically authorized by the Director General under subsection (1) may obtain from a Magistrate's Court, a search warrant for the purpose of entering such premises and exercising all or any of the powers conferred upon such officer by such search warrant.

(4) Notwithstanding the provisions of subsection (1), the Authority or any other officer authorized in writing in that behalf by the Authority may without a warrant excise all or any of the powers referred to in that subsection, if, in the opinion of the Authority, –

(a) the investigation needs to be conducted urgently since it would likely to have serious impact on public health, public safety, privacy, national security, international stability or on the effective functioning of the government or the economy of Sri Lanka; and

(b) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible.

(5) As soon as may be practicable the Authority shall and in any event within seventy-two hours of such action which was carried out without a warrant, make an application to the Magistrate to have such action confirmed.

Authority to be a scheduled institution within the meaning of the Bribery Act (Chapter 26)

29. For the purpose of this Act, the Authority shall be deemed to be a scheduled institutions within the meaning of the Bribery Act (Chapter 26) and the provisions of that Act, shall be construed accordingly.

Members of the Board and officers and servants of the Authority deemed to be public servants

30. For the purpose of this Act all members of the Board, officers and servants of the Authority shall be deemed to be public servants within the meaning and for the purposes of the Penal Code (Chapter 19)

Acquisition of immovable property under the Land Acquisition Act

31. (1) Where any immovable property is required to be acquired for any specific purpose of the Authority and the Minister by Order published in the *Gazette* approves of the proposed acquisition for that purpose that property shall be deemed to be required for a public purpose and may accordingly be acquired under the Land Acquisition Act and transferred to the Authority.

(2) Any sum payable, for the acquisition of any immovable property under the Land Acquisition Act for the Authority shall be paid out of the Fund of the Authority.

Expenses in suit or prosecution to be paid out of the Fund

32. (1) Any expense incurred by the Authority in any suit or prosecution brought by or against it before any Court, shall be paid out of the Fund and any costs paid to or recovered by the Authority in any such suit or prosecution shall be credited to the Fund.

(2) Expenses incurred by any member of the Board, or any officer or employee of the Authority in any suit or prosecution brought against him before any court or tribunal in respect of any act which is done or purported to be done by him under the provisions of this Act or any other written law or if the court holds that such act was done in good faith, be provident of the Fund, unless such expenses are recoverable by him in such suit or prosecution.

Annual report

33. (1) The Authority shall within six months of the end of each financial year, submit to the Minister an annual report of the activities carried out by the Authority during that financial year, and cause a copy each of the following documents to be attached to the report –

(a) the audited accounts of the Authority for the year along with the Auditor-General's report;

(b) report on the activities carried out by the Authority during the preceding year; and

(c) a report of proposed activities for the year immediately following, the year to which such report and accounts relate.

(2) The Minister shall lay copies of the report and documents submitted under subsection (1) before Parliament within six months from the date of receipt of such report.

Directions by the Minster

34. (1) The Minister may, from time to time, advise the Authority informing changes in the government policy, and it shall be the duty of the Authority to give effect to such directions in discharge of its powers, duties and functions.

(2) The Minister may direct the Authority to furnish to him in such form as he may require, returns, accounts and any other information relating to the work of the Authority, and it shall be the duty of the Authority to give effect to such directions.

Duty to maintain confidentiality

35. The Authority, or any other institution, entity or person who obtains information under this Act shall, maintain confidentiality and observe strict secrecy respecting all matters of which such information provided as designated as confidential, and shall not disclose any information which may come to his knowledge in the exercise, performance and discharge of his power, duties and functions under this Act, except -

(a) where it is necessary to comply with any provision of this Act or any rule or regulation made thereunder or any other written law;

(b) upon an order of a court of law; or

(c) where such disclosure is necessary in the interest of national security, public interest or to safeguard the interest of individuals.

Rules

36. (1) The Authority shall make rules in respect of –

(a) the schemes of recruitment, terms of appointment, employment and dismissal of various officers and employees and their powers, functions including the

conditions of employment of the Director General and the payment of remuneration;

(b) the procedure to be observed at the summoning and holding of meetings of the Authority;

(c) the management of the affairs of the Authority; and

(d) other matters for which rules are required to be made under this Act.

(2) Every rule made by the Authority shall be approved by the Minister and be published in the *Gazette* and shall come into operation on the date of its publication or on such later date as may be specified therein.

Regulations

37. (1) The Minister may make regulations with the concurrence of the Authority in respect of any matter required by this Act to be prescribed or in respect of which regulations are authorized by this Act to be made.

(2) In particular and without prejudice to the generality of the powers conferred by subsection (1), the Minister may make regulations for and in respect of all or any of the following matters specifying: -

(a) the duties and responsibilities of the Owners of CNIIs;

(b) the policies, standards, and guidelines to be adhered by the CNIIs, government institutions and other relevant sectors for protecting computer, computer program, computer systems, and related devices;

(c) the conditions in relation to the compliance with the cyber security policies, procedures, standards and guidelines by CNIIs, government institutions, and other relevant sectors and form and manner of reporting such information to the Authority;

(d) information on cyber security threats and incidents required by the Authority from sectoral CERTs and CSIRTs, ISPs, Lanka Domain Registry, law enforcement authorities

or any other relevant institution, and form and manner of reporting such information to the Authority;

(e) duties and responsibilities of the Information Security Officer appointed by the Authority;

(f) procedures and conditions for the grant and renewal of accreditation, the validity of accreditation, revocation or suspension of accreditation in relation to cyber security service;

(g) procedures and timelines for conducting cyber security risk assessments, audits other relevant assessments by CNIIs, government institutions, and relevant sectors; and

(h) specifying the fees and charges levied for any service provided under this Act.

(3) Every regulation made under this section shall be published in the *Gazette* and shall come into operation on the date of such publication or on such later date as may be specified in that regulation.

(4) Every regulation made under this section shall within three months after its publication in the *Gazette,* be brought before Parliament for approval.

(5) Every notification specifying the date on which the Parliament has approved the regulation shall be published in the *Gazette*. Any regulation which is not so approved shall be deemed to be rescinded as from the date of such disapproval but without prejudice to anything duly done thereunder prior to such disapproval.

(6) The notification specifying the date on which any regulation is deemed to be so rescinded shall be published in the *Gazette.*

Interpretation

38. In this Act, unless the context otherwise requires –

"CERT" means computer emergency readiness team which is an organization that handles computer security incidents. Alternative names for such groups include computer security incident response team (CSIRT)

"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 system" means a group of interconnected computers or related devices which are used to collect, process, store, maintain, use, share, and disseminate information. It includes information system designed to perform a specific function, a cloud-based system, intra or Internet based system, Internet of Things, and operational technology systems such as industrial control systems;

"computer program" means a set of instructions that can be executed by the computer or related device to achieve the intended result. This also includes virtual assets such as application software, websites, database, digital documents and any other information processing application;

"cyber security" refers to the protection of information in transit, in process and in storage, being used by computer, computer program, computer system or related devices from any form of attacks, or unauthorized access, use, disclosure, disruption, modification or destruction. This also includes any set of activities intended to make cyberspace safe and secure;

"cyber security threat" means any circumstance, or known or suspected activity that could be potentially harmful or have an adverse impact on a computer, computer program, computer system or related devices that may affect the cyber security of that computer, computer program, computer system or device;

"cyber security incident" means any act or activity carried out without lawful authority on a computer, computer

system or related devices that may affect the cyber security of the that computer, computer program, computer system or device;

"Critical National Information Infrastructure" means, the computer, computer program, computer system, or related device identified by the Authority as a Critical National Information Infrastructure under this Act, which is located wholly or partly in Sri Lanka, and its disruption or destruction would create a serious impact on the national security, public safety, public health and economic wellbeing of citizens, delivery of essential services or effective functioning of the government or the economy of Sri Lanka;

"civilian aspects of cyber security" means any cyber security activity related to public and private domains other than military domain;

"cyber security service provider" means an individual or organization which provides services to ensure the cyber security of a computer, computer program, computer system or any related device of a client organization. A list of cyber security services pertaining to this Act is presented in <PART VIII>;

"Defence Cyber Command (DCC)" means the organization established under the Defence Cyber Command Act, No. of 2023;

"device" means any equipment, static or mobile, which uses information and communication technology to perform it's general or specific tasks;

"information" includes data, text, images, sound, codes, computer program, or databases. It may in the forms of electronic, digital or physical formats;

"Minister" means the Minister assigned the subjects and functions relating to cyber security under Article 43 or 44 of the Constitution;

"National Information and Cyber Security Strategy" includes Information and Cyber Security Strategies made from time to time;

"Officials accountable for CNII means –

(a) the head of a government department or institution, or a corporation established by or under any written law;

(b) every director and any other officer of a body corporate responsible for the CNIIs;

(c) every partner of a firm responsible for the CNIIs; or

(d) every officer responsible for CNIIs in an unincorporated body; and

"prescribed" means prescribed by regulations under this Act.

Sinhala text to prevail in case of inconsistency

39. In the event of any inconsistency between the Sinhala and Tamil texts of this Act, the Sinhala text shall prevail.