L.D.O. 14/2019

AN ACT TO PROVIDE FOR THE IMPLEMENTATION OF THE NATIONAL CYBER SECURITY STRATEGY OF SRI LANKA, TO PROVIDE FOR THE ESTABLISHMENT OF THE CYBER SECURITY AGENCY OF SRI LANKA, TO PROVIDE FOR THE EMPOWERMENT OF THE SRI LANKA COMPUTER EMERGENCY READINESS TEAM AND NATIONAL CYBER SECURITY OPERATIONS CENTRE, TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE WITHIN 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 2019.

(2) The provisions of this Act except the provisions of Part VII, shall come into operation on the date on which the certificate of the Speaker is endorsed in respect of this Act in terms of Article 79 of the Constitution.

(3) 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*.

PART I

OBJECTIVES OF THE ACT

Objectives of the Act

2. The Objectives of the Act shall be -

(a) to ensure the effective implementation of the National Cyber Security Strategy in Sri Lanka;

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

(c) to establish the Cyber Security Agency of Sri Lanka and to empower other institutional framework to provide for a safe and secure cyber security environment; and

(d) to protect the Critical Information Infrastructure.

PART II

CYBER SECURITY AGENCY OF SRI LANKA

Establishment of the Cyber Security Agency

3. (1) There shall be established an agency which shall be called the Cyber Security Agency of Sri Lanka (hereinafter referred to as ‘‘the Agency’’) for the purposes of this Act .

(2) The Agency 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.

(3) The Agency shall be the Apex and Executive body for all matters relating to cyber security policy in Sri Lanka and shall be responsible for the implementation of the National Cyber Security Strategy of Sri Lanka.

Powers, duties and functions of the Agency

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

(a) take all necessary steps to implement the National Cyber Security Strategy of Sri Lanka including preparation and execution of operational strategies, policies, action plans, programs and projects;

(b) develop cyber security policies and standards for the government of Sri Lanka, to facilitate the adoption of the policies and standards in all government institutions and other relevant sectors and prescribe an assessment framework and criteria to assess cyber security policies and standards ;

(c) identify and designate Critical Information Infrastructure (hereinafter referred to as "the CII") both in government and other relevant sectors, in consultation with relevant stakeholders;

(d) develop strategies and plans for the protection of CII in consultation with the owners of CII;

(e) act as the central point of contact for cyber security in Sri Lanka, and provide all necessary advice to all government institutions and other relevant sectors in respect of cyber security matters;

(f) act as the interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cyber security risks, incidents, analysis, and warnings in relation to cyber security for

government institutions and other relevant sectors ;

(g) enter into agreements with other apex institutions for cyber security in respect of any cyber security policy related matters and to represent Sri Lanka at international level in such matters;

(h) to assist in the curricular, and skills development relating to cyber security including the development of cyber security industry standards to ensure the availability of competent and highly skilled professionals in cyber security domain;

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

(j) establish or designate institutions, units or any other entity to assist the Agency in the performance and discharge of the duties and functions of the Agency ;

(k) establish and authorize sectoral computer emergency readiness teams in various sectors based on the critical importance of a particular sector;

(l) to request the submission of reports or returns from the owners of the designated CIIs and other government institutions which includes information relating to the compliance with the cyber security assessment and information relating to the steps taken to protect their CIIs ;

(m) to promote the awareness of citizens regarding the risks in cyberspace, and build the capacity to protect their identity, privacy, and economic assets in cyber space;

(n) 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 in accordance with the provisions of this Act, any such movable or immovable property of the Agency;

(o) open and maintain bank accounts with any bank as determined by the Agency and authorize any person to operate such account or accounts on behalf of the Agency;

(p) receive grants or contributions from any sources whatsoever and to raise funds by all lawful means and apply such funds in the performance and discharge of the duties and functions of the Agency;

(q) make rules in respect of the matters for which rules are required to be made under the Act; and

(r) do all such other acts which are not inconsistent with the provisions of this Act as may be expedient for the accomplishment of the objects of the Agency.

(2) In the discharge of its powers and functions, the Agency shall at all times consult Sri Lanka Computer Emergency Readiness Team and ensure the said powers are carried out through the institutions established under Part IV of this Act.

(3) The Agency shall, for the purpose of giving effect to the provisions of this Act, in consultation with the Head of a Government Institution or Department designate an officer of such institution or Department as an Information Security Officer (hereinafter referred to as the "ISO") in accordance with such criteria as may be determined by the Agency.

(4) Every ISO shall ensure the government Institution's or Department's compliance with such prescribed standards relating to cyber security.

Constitution of the Board

5. (1) The management and administration of the affairs of the Agency shall be vested in a Board of Directors (hereinafter referred to as the "Board" which shall consist of –

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

(i) the Secretary to the Ministry of the Minister to whom the subject of Defense is assigned or an additional Secretary of such Ministry nominated by the Secretary ;

(ii) the Secretary to the Ministry of the Minister to whom the subject of Public Administration is assigned or an additional Secretary of such Ministry nominated by the Secretary ;

(iii) the Secretary to the Ministry of the Minister to whom the implementation of this Act is assigned or an additional Secretary of such Ministry nominated by the Secretary ;

(iv) a member nominated by the Board of Sri Lanka Computer Emergency Readiness Team; and

(b) three members appointed by the Minister, (hereinafter referred to as "appointed members") each of whom have over 25 years' experience and have demonstrated professional excellence in the fields of Information and

Communication Technology, Public or Private sector Management, Law or Finance.

(2) The Minister shall, in consultation with the Board appoint one of the appointed members to be the Chairman of the Board.

(3) Where the Chairman is temporarily unable to perform his duties of his office due to ill health, absence from Sri Lanka or for any other reason, the Minister may appoint any other member to act as the Chairman in addition to his normal duties as a member.

(4) The Minister shall, prior to appointing a person as a member of the Agency, satisfy himself that such person has no financial or other conflict of interest in the affairs of the Agency, as is likely to affect adversely, the discharging of his functions as a member of the agency.

(5) The Minister shall also satisfy himself, from time to time, that no member of the Agency has since being appointed acquired any such interest referred to in subsection (4).

(6) A member of the Agency who is in any way, directly or indirectly interested in any contract made or proposed to be made by the Agency shall disclose the nature of his interest at a meeting of the Agency and such disclosure shall be recorded in the minutes of the Agency and the member shall not participate in any deliberation or decision of the Agency with regard to that contract.

Disqualifications from being a member of the Board

6. A person shall be disqualified from being appointed or from continuing as a member if he -

(a) is or becomes a member of parliament, member of provincial council or a member of local Authority; or

(b) is or becomes directly or indirectly, by himself or by any other person on his behalf, holds or enjoy any right or benefit under any contract made by or on behalf of the Agency as the case may be;

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

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

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

Meetings of the Board

7.(1) The Chairman shall preside at every meeting of the Board. In the absence of the Chairman from any meeting of the Board, the members present shall elect one among their members to preside at such meeting.

(2) The quorum for any meeting of the Agency shall be four members.

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

(4) Subject to the preceding provisions of this section, the Board may regulate the procedure in relation to the meetings of the Board and the transaction of business at such meetings by way of rules published in the *Gazette*.

Seal of the Agency

8. (1) The seal of the Agency -

(a) shall be in the custody of such person as the Board may decide 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 Agency has been affixed.

Acts not invalidated by reason of vacancy or defect in appointment

9. No act, decision or proceeding of the Board shall 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.

Remuneration of members

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

Term of office of the appointed members

11. (1) Every appointed member shall, unless he vacates office earlier by death, resignation or removal, hold office for a term of three years from the

date of his appointment and shall unless he has been removed, be eligible for reappointment.

(2) The Minister may, if he considers it expedient to do so, remove from office any appointed member after assigning reasons therefor.

(3) Any appointed member may at any time resign his office by letter to that effect addressed to the Minister and sent by registered post.

(4) In the event of vacation of office by death, resignation or removal of any appointed member, the Minister may having regard to the provisions of section 5(b), appoint any other person to succeed such member. Any member so appointed shall hold office for the unexpired term of office of the member whom he succeeds.

(5) Where an appointed member, by reason of illness, infirmity or absence from Sri Lanka for a period of not less than three months, is temporarily unable to perform his duties, it shall be the duty of such member to inform the Minister in writing of such inability. The Minister may, on receipt of such information, having regard to the provisions of section 5(b), appoint some other person to act in his place.

PART III

APPOINTMENT OF THE DIRECTOR GENERAL AND STAFF OF THE AGENCY

Appointment of the Director General

12. (1) The Agency shall in consultation with the Minister, appoint a person as a Director General of the Agency in accordance with such scheme of recruitment formulated by the Agency with the approval of the Ministry of Finance.

(2) The scheme of recruitment referred to in subsection (1) shall include as qualifications for the post of a Director General,

(a) a post graduate degree in the field of science or engineering; and

(b) ten years of experience in a senior executive level in cyber security or related field.

(3) The Director General appointed under subsection (1) shall be the Chief Executive Officer of the Agency.

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

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

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

(c) exercise such powers and functions of the Agency under this Act as may be assigned to him by the Board;

(d) function as the Secretary to the Board.

(5) The term of the office of the Director General appointed under subsection (1) 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 shall becomes vacant upon the death, removal from office or resignation by letter in that behalf addressed to the Board of the Agency by the holder of that office, the Agency

may appoint any other senior officer of the Agency to perform the duties of the Director General until an appointment is made under subsection (1).

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

(8) The Director General shall hold office in accordance with the terms of his appointment and there shall be paid to him such remuneration as is determined by the Minister, out of funds of the Agency in consultation with the Minister assigned the subject of Finance.

(9) The Director General may be removed from office by the Agency in the event that he –

(a) becomes permanently incapable of performing his duties;

(b) has done any act which is of a fraudulent or illegal character or is prejudicial to the interest of the Agency; or

(c) has failed to comply with any directions issued by the Agency.

(10) The Director General may with the approval of the Board, delegate to an officer of the Agency, 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.

Other officers and employees of the Agency

13. (1) The Agency may appoint such number of officers and employees as it may consider necessary for the efficient exercise and performance of its powers, and functions under this Act.

(2) In appointing officers and employees as it may consider necessary, the Agency shall obtain service of persons possessing proven experience and who

have shown capacity in the areas relating to cyber security or any other related area as may be determined by the Agency to assist in the exercise or performance of its powers and functions under this Act.

(3) The Agency shall exercise disciplinary control over such officers and employees.

(4) The officers and employees shall be remunerated in such manner and at such rates in consultation with the Minister assigned the subject of Finance and shall be subject to such conditions of service as may be determined by the Agency.

Appointment of public officers to the staff of the Agency

14. (1) At the request of the Agency any officer in the public service may, with the consent of that officer and the Public Service Commission, be temporarily appointed to the staff of the Agency for such period as may be determined by the Board 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 Agency, 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 him.

(3) Where any officer in the public service is permanently appointed to the staff of the Agency, 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 him.

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

PART IV

INSTITUTIONAL FRAMEWORK TO ASSIST THE AGENCY

Sri Lanka Computer Emergency Readiness Team

15.(1) The Sri Lanka Computer Emergency Readiness Team, incorporated as a Company under the Companies Act No. 7 of 2007 (herein after referred to as "the CERT") shall be the national point of contact for cyber security incidents in Sri Lanka.

(2) The CERT shall at all times assist the Agency in the exercise, performance and discharge of its powers and functions under this Act.

(3) In addition to the powers and functions set out in its Articles of Association, CERT shall have the following powers and functions:-

(a) to function as the National Computer Emergency Readiness Team of Sri Lanka and the coordination center for cyber security incidents and responses between the CERT and sectoral Computer Emergency Readiness Teams authorized by the Agency ;

(b) to act as the National Point of Contact for handling cyber security incidents;

(c) to conduct reactive cyber security services through timely responses to cyber security incidents and mitigate the resulting damage;

(d) to conduct proactive services to prevent incidents through awareness building, research and training;

(e) to provide the necessary technical assistance to law enforcement agencies in digital forensic investigations;

(f) to provide timely technical assistance on cyber security issues upon the request of any government institution or other relevant sectors;

(g) to conduct and manage cyber security services for government institutions and other sectors, on request;

(h) to share cyber threat intelligence with the government institutions , other sectors and members of the public in a timely manner;

(i) to provide national level cyber threat intelligence information to the Agency;

(j) to establish and maintain membership, collaborate with International Computer Emergency Readiness Teams and related bodies in order to ensure effective coordination and response to cyber security related incidents in Sri Lanka.

National Cyber Security Operations Centre

16.(1) There shall be a National Cyber Security Operations Centre (hereinafter referred to as "NCSOC") designated by the Minister for the purpose of this Act.

(2) In designating the NCSOC the Minister may, with the concurrence of the Agency by Order published in the *Gazette*, designate the CERT or any institution, unit, entity established by the Agency, which shall be charged with the implementation of the provisions of this section.

(3) The Minster shall, in making the Order referred to in subsection (2) take into consideration the capacity and competency in relation to its overall ability to discharge the powers and functions of a NCSOC.

(4) The NCSOC shall render all assistance as shall be required by the Agency in the exercise of its powers and the discharge of its functions under this Act.

(5) The powers and functions of the NCSOC shall be:-

(a) to identify potential cyber security incidents in a proactive manner and facilitate coordinated response to cyber security incidents;

(b) to monitor the designated CIIs owned by the government and other sectors in order to detect, investigate, and respond to potential cyber threats;

(c) to gather cyber threat intelligence information from local and international sources;

(d) to provide cyber threat intelligence information to law enforcement authorities, CERT and to the Agency to prevent cyber security incidents.

Minister to seek assistance of other institutions to assist the Agency

17. The Minister may, on the recommendation of the Agency and CERT, and having regard to the necessity, interests of the national security, national economy and public order or any other similar situation which necessitate assistance of other institutions request such institution to provide assistance to the Agency in the exercise, performance of powers and functions of the Agency.

PART V

CRITICAL INFORMATION INFRASTRUCTURE

Designation of a computer or computer system as CII

18. (1) The Agency shall identify and recommend to the Minister the designation of a computer or computer system as CII for the purposes of this Act, if the Agency is satisfied that-

(a) the computer or computer system is necessary for the continuous delivery of essential services for the public health, public safety, privacy, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace or for any other criteria as may be prescribed and the disruption or destruction of which would likely to have serious impact on the public health, public safety, privacy, national security, international stability or on the effective functioning of the government or the economy; and

(b) the computer or computer system is located wholly or partly in Sri Lanka; and

(2) The Agency shall prior to making recommendation under subsection (1), obtain the concurrence of any prescribed regulatory or supervisory institution established under any written law which regulates or supervise the designated CIIs for the purpose of subsection (1).

(3) The designated CII may be owned or operated by the government institutions or other institutions.

(4) On the recommendation of the Agency under subsection (1), the Minister shall, by Order publish in the *Gazette*, designate such recommended computer or computer system as CII.

(5) The order published in the *Gazette* under subsection (3) shall -

(a) identify the computer or computer system that is being designated as a CII;

(b) identify the owner of the computer or computer system so designated as a CII;

(6) For the purposes of this Act, the head of the organization responsible for the CII shall be deemed to be the "owner" of the CII .

(7) The Agency may recommend to the Minister, to withdraw the designation of any CII at any time, if the Agency is of the opinion that the computer or computer system no longer fulfils the criteria of a CII as stipulated under subsection (1).

(8) Upon receiving such recommendation under subsection (7), the Minister shall withdraw the designation of the computer or computer system as a CII by order published in the *Gazette*.

Obligations of the owner of the CII

19. (1) Upon the designation of a computer or computer system as CII, the owner of the CII shall -

(a) be responsible for the protection of CII, and take all necessary steps to protect CIIs as may be prescribed.

Provided that, if the CII spreads across multiple organizations or multiple sectors, all the heads of such organizations or sectors shall become jointly and severally responsible for protection of the CII.

(b) be responsible -

(i) for developing and implementing protection plan for securing the CII;

(ii) for facilitating the Agency or any other institution, unit or entity established or designated by the Agency to perform the duties and functions of the Agency under this Act;

(iii) for adopting policies, procedures and standards prescribed for securing the CII;

(c) conduct security risk assessments, audits and vulnerability assessments of the CII, in compliance with the procedures and timelines, as may be determined by rules under this Act.

(d) furnish the information on the design, configuration, security and such other technical details or information relating to the operations of the CII or any other interconnected computer or computer systems under the control of the owner, to the Agency in the form, manner and within the period of time as may be determined by rules ;

(e) furnish any other information which may be required to ascertain the level of cyber security of the CII to the Agency, in the form, manner and within the period of time

as may determined by rules; and

(f) notify the Agency and CERT of the occurrence of any cyber security incident in respect of the designated CII or any other interconnected computer or computer system under the control of the owner, in the form and manner as may be prescribed not later than 24 hours after becoming aware of such occurrence.

PART VI

FUND OF THE AGENCY

Fund of the Agency

20. (1) The Agency 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 by Parliament for the use of Agency out of the Consolidated Fund.

(b) all such sums of money as may be received by the Agency 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 Agency by way of gifts, grants or donations from any source.

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

written law an all such sums as are required to be paid out of the Fund.

PART VII

OFFENCES AND PENALTIES

Offences and Penalties

21. (1) Every person who being the owner of a CII who fails, without reasonable cause, to fulfill the obligations imposed under this Act or fails to report cyber security incidents to the Agency and CERT, in accordance with section 19(1) (c) to (f), commit an offence under this Act and shall on conviction be liable to a fine not exceeding two hundred thousand rupees or to imprisonment for a term not exceeding two years or to both such fine and imprisonment.

(2) An ISO who fails to perform duties and responsibilities relating to cyber security prescribed under this Act, shall commit an offence:

Provided that, no person shall be deemed guilty of that offence if such person proves that such offence was committed without his knowledge, consent or connivance or that he exercised all due diligence to prevent the commission of such offence.

(3) Every person who being a head of an institution other than of a designated CII fails to facilitate an ISO for the proper discharge of the duties and responsibilities prescribed under this Act, shall commit an offence:

Provided that, no person shall be deemed guilty of that offence if such person proves that such offence was committed without his knowledge consent or connivance or that he exercised all due diligence to prevent the commission of such offence.

(4) A prosecution under this Act shall be instituted by the Agency or an

officer authorized by the Agency.

(5) Upon any conviction under subsection (1), the Agency shall take steps to publish the names of the persons in the print or electronic media as the case may be, for public information.

(6) For the purpose of this section "person " shall include a body corporate, a firm, a statutory authority, government department.

Offences committed by a body of persons

22. Where an offence under this Act is committed by a body of persons, then –

(a) if that body corporate, every director or officer of that body corporate; and

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

shall commit an offence:

Provided that, no such director, officer or partner shall be deemed guilty of that offence if he proves that such offence was committed without his knowledge or that he exercised due diligence to prevent the commission of such offence.

PART IX

MISCELLANEOUS

Financial year and audit of accounts

23. (1) The financial year of the Agency shall be the calendar year.

(2) The provisions of Article 154 of the Constitution relating to the audit of the accounts of public corporations and the provisions of sections 40 and 41 of the National Audit Act, No.19 of 2018, shall apply to the audit of the accounts of the Agency.

Power of entry, inspection and search

24. The Agency or any other officer authorized in writing in that behalf by the Agency, for the purpose of ascertaining whether the provisions of this Act or any regulation made thereunder are being complied with may, on reasonable ground -

(a) enter, inspect and search premises of the designated CIIs;

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

(c) examine any person whom he has reasonable cause to believe that such person is an owner or employee of such CII.

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

25. For the purpose of this Act –

(a) the Agency; and

(b) the CERT and the NCSOC,

shall be deemed to be a scheduled institution within the meaning of the Bribery Act (Chapter 26) and the provisions of that Act, shall be construed accordingly.

Members, officers and servants of the Agency deemed to be public servants

26. For the purpose of this Act –

(a) all members of the board, officers and servants of the Agency; and

(b) all officers and servants of the CERT and NCSOC,

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

27. (1) Where any immovable property is required to be acquired for any specific purpose of the Agency 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 Agency.

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

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

28. (1) Any expenses incurred by the Agency 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 Agency in any such suit or prosecution shall be credited to the fund.

(2) Expenses incurred by any member, or any officer or employee of the Agency 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

29. (1) The Agency shall within six months of the end of each financial year, submit to the Minister an annual report of the activities carried on by the Agency 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 Agency for the year along with the Auditor-General's report;

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

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

(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 Minister

30. (1) The Minister may from time to time, issue to the Agency such general or special directions in writing as to the exercise and performance of its powers and functions so as to ensure the giving proper effect to Government policy and it shall be the duty of the Agency to give effect to such directions.

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

Rules

31. (1) Subject to the provisions of this Act, the Agency may make rules in respect of all matters for which rules are authorized or required to be made under this Act.

(2) Every rule made by the Agency 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

32. (1) The Minister may make regulations with the concurrence of the Agency 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 criteria for the designation of the CII;

(b) the duties and responsibilities of the owners of CII;

(c) the standards and procedures based on the cyber security policy to be adhered by the government and protection plans for computer or computer systems by government institutions;

(d) the standards for accrediting the cyber security training program and training institutes;

(e) the procedures to connect with NCSOC;

(f) the standards for accrediting cyber security auditors;

(g) the procedures and timelines for conducting cyber security risk assessments;

(h) the procedure and timelines for conducting security audits and vulnerability assessments for CII;

(i) form and manner of reporting cyber security incidents and cyber threat intelligence information to Agency by CERT;

(j) duties and responsibilities of the ISOs appointed by the agency;

(k) form and manner of reporting cyber security incidents to CERT by all the government institutions and other relevant sectors;

(l) form and manner of reporting cyber security incidents to CERT by all the sectoral CERTs and any other CERTs;

(m) policies, procedures and standards for securing computers, computer systems or any other digital infrastructure of all the government institutions;

(n) the conditions in relation to the compliance with the cyber security policy by all government institutions;

(2) Every regulation made under subsection (1) and (2) 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 the regulation.

(3) Every regulation made under subsection (1) shall, forthwith after its publication in the *Gazette* be brought before Parliament for approval and 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 previously done thereunder.

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

Interpretation

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

"Automatic" means without directed intervention;

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

"computer programe" means a set of instructions that can ne executed by the computer to achieve the intended result;

" Cyber security" means a set of activities intended to make cyber space safe and secure;

" Minister" means the Minister assigned the subjects and functions relating to cyber security.

"Processing data" means that data in the computer system is operated by executing a computer programe.

Sinhala text shall prevail

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

22/05/19