

**AN ACT TO PROVIDE FOR THE IMPLEMENTATION OF THE NATIONAL CYBER SECURITY STRATEGY OF SRI LANKA; TO PROVIDE FOR THE ESTABLISHMENT OF THE DIGITAL INFRASTRUCTURE PROTECTION AGENCY OF SRI LANKA; TO PROVIDE FOR THE EMPOWERMENT OF THE SRI LANKA COMPUTER EMERGENCY READINESS TEAM AND OTHER INSTITUTIONAL FRAME WORK; 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 commence 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 as may be approved by the Cabinet of Ministers;
- (b) to prevent, mitigate and respond to cyber security threats and incidents effectively and efficiently;
- (c) to provide for a safe and secure cyber security environment; and
- (d) to protect the Critical Information Infrastructure.

## **PART II**

### **DIGITAL INFRASTRUCTURE PROTECTION AGENCY OF SRI LANKA**

**Establishment  
of the Agency**

3. (1) There shall be established an agency which shall be called the Digital Infrastructure Protection 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 executive body for the implementation of all matters relating to cyber security in 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 as may be approved by the Cabinet of Ministers including preparation and execution of operational strategies, action plans, programs and projects;

- (b) recommend cyber security policies and standards for the government of Sri Lanka and to facilitate the implementation of the policies and standards in all government institutions and other relevant sectors and determine 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 CIIs in consultation with the owners of CIIs;
- (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 or engage in any activity, either alone or in conjunction with other apex government or regulatory institutions or international agencies or organizations, responsible for cyber security in Sri Lanka and in other foreign states for the purposes of this Act;

- (h) represent Sri Lanka internationally in matters relating to cyber security with the approval of the Minister;
- (i) assist in the curricular, and skills development relating to cyber security including the development of standards of cyber security industry to ensure the availability of competent and highly skilled professionals in cyber security domain;
- (j) coordinate the conduct of sectoral cyber security drills from time to time to improve overall cyber security readiness;
- (k) 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 in consultation with the relevant Minister ;
- (l) establish and authorize sectoral computer emergency readiness teams in various sectors in accordance with such criteria and procedures as may be prescribed based on the critical importance of a particular sector;
- (m) 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 standards and information relating to the steps taken to protect their CIIs ;
- (n) promote the awareness of citizens regarding the risks in cyber space, and build the capacity to protect their identity, privacy, and economic assets in cyber space;

- (o) require the institutions where an Information Security Officer has been designated under subsection (3), to take appropriate measures as may be prescribed to protect and safeguard computer systems or computer programs, based on the rules made under this Act and directives as may be determined;
- (p) 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;
- (q) 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;
- (r) receive grants or contributions from any source 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;
- (s) make rules and issue directives in respect of the matters for which rules and directives are required to be made or issued under the Act;
- (t) impose such charges and levies for any service rendered by the Agency; and
- (u) 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 Agency.

(2) (a) The Agency may, in the discharge of its powers and functions direct the Sri Lanka Computer Emergency Readiness Team (hereinafter in this Act referred to as “the CERT”) to provide such technical and other assistance as may be required by the Agency.

(b) The Sri Lanka Computer Emergency Readiness Team shall comply with such directions issued by the Agency for the purpose of paragraph (a).

(3) The Agency shall, for the purpose of giving effect to the provisions of this Act, in consultation with the owner of the Critical Information Infrastructure, designate an officer of such CII as an Information Security Officer (hereinafter referred to as the “ISO”) in accordance with such criteria as may be prescribed.

(4) Every ISO designated under subsection (3) shall ensure the compliance with such rules made under this Act and directives issued by the Agency from time to time relating to cyber security matters.

**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 Defence 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 or an additional Secretary of such Ministry nominated by the Secretary ; and

(b) four members appointed by the Minister, (hereinafter referred to as “appointed members”) each of whom have over fifteen years experience and have demonstrated professional excellence in the fields of cyber security, 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 Agency.

(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 Board shall 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 Board, 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 Board.

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

(6) A member of the Board who is in any way, directly or indirectly interested in any contract made or proposed to be made by the Board shall disclose the nature of his interest at a meeting of the Board and such disclosure shall be recorded in the minutes of the Board and the member shall not participate in any deliberation or decision of the Board 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;
- (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;
- (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;  
or
- (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 published in the *Gazette* by way of rules made under this Act.

**Seal of the  
Agency**

**8.** (1) The seal of the Agency -

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

**Acts not  
invalidated by  
reason of**

**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.

**vacancy or  
defect in  
appointment**

**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(1)(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(1)(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 of eminence and integrity and who is not a member of any political party as a Director General of the Agency in accordance with such scheme of recruitment formulated by the Agency with the approval of the Minister assigned the subject of Finance.

(2) The scheme of recruitment referred to in subsection (1) shall include the following requirements as qualifications for the holder of the post of Director General -

- (a) bachelors degree or equivalent in the field of Science, Engineering, Management, Law or a related field; and
- (b) a post graduate degree or equivalent in the field of Science, Engineering, Management, Law or a related field; and
- (c) ten years of experience in a senior executive level in the field of cyber security, information technology or in a 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 Board –

- (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 Board;
- (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 office of the Director General appointed under subsection (1) hold office for a period of four 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 by the holder of that office, the Board 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 the fund 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 rules made under this Act or directives 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, duties 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 (hereinafter in this Act referred to as “the CERT”) incorporated as a Company under the Companies Act, No. 7 of 2007 shall be the national coordination point of contact for cyber security incidents and threats 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) The CERT shall not sell or otherwise dispose of its shares in any manner without the approval of the Agency.

(4) In addition to the powers and functions set out in its Articles of Association, the 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 conduct reactive cyber security services through timely responses to cyber security incidents and mitigate the resulting damage and facilitate coordinated response to cyber security incidents;
- (c) to conduct proactive services to prevent incidents through awareness building, research and training;
- (d) 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 relevant sectors, on request;
- (h) to share cyber threat information with the government institutions , other relevant sectors and members of the public in a timely manner;

- (i) to provide national level cyber threat 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; and
- (k) to monitor the designated CIIs owned by government and other relevant sectors in order to detect, investigate and respond to potential cyber threats, in accordance with such rules incorporating adequate safeguards ensuring fairness of the monitoring made under this Act.

**Minister to seek assistance of other institutions in the event of national security etc**

**16.** The Minister in consultation with the Secretary to the Ministry of the Minister assigned the subject of defence and having regard to the necessity, interests of the national security, national economy and public order or the existence of any other similar situation, require the sectoral computer emergency readiness teams, established under paragraph (l) of section 4(1) and designated CIIs, to assist and submit such information as may be necessary in the exercise, performance and discharge of powers and functions of the Agency and the CERT under this Act, or on an Order made by a competent court.

## **PART V**

### **CRITICAL INFORMATION INFRASTRUCTURE**

**Designation of a computer or computer system as CII**

**17.** (1) The Agency shall identify and designate of an institution having a computer system or computer program as an Institution having a CII, by Order published in the *Gazette* if the Agency has reasonable grounds to believe that-



(a) the disruption or destruction of the computer system or computer program would have serious impact on the national security, public health, public safety, confidentiality, or economic well – being of citizens, or the effective functioning of the government or the economy of Sri Lanka; and

(b) the computer program or the computer system is located wholly or partly in Sri Lanka.

(2) The Agency shall prior to designating an Institution as CII under subsection (1), obtain the concurrence of any regulatory or supervisory institution established under any written law which regulates, authorizes or supervises the institution sought to be designated as CII.

(3) The institution designated as CII may be a government institution or any other institution including private sector institutions.

(4) The order published in the *Gazette* under subsection (1) shall -

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

(b) identify the owner of and the functions of the CII;

(5) The Agency shall provide an opportunity for an owner of a CII to adduce reasons why its computer programme or computer system shall not be designated as a CII or request the withdrawal of the designation of a CII.

(6) Subject to subsection (5), where an institution is designated as CII, the owner of such CII being aggrieved by the decision of the Agency referred to in subsection (1), may prefer an appeal to the Secretary of the Minister within thirty days from the date of publication of the Order specified in subsection (4).

(7) The Secretary to whom an appeal is preferred under subsection (6) shall within 14 days thereafter conduct an inquiry, providing an opportunity for the owner of the CII and the Agency to be heard, and thereafter make a decision taking into consideration the reasons adduced by the Agency to designate a CII and shall either –

- (a) allow the appeal and direct the Agency to revoke its decision to designate such institution as CII; or
- (b) disallow the appeal for reasons assigned.

(9) The Agency shall give effect to the decision of the Secretary made under subsection (8).

(10) The Agency may withdraw the designation of any CII at any time by Order published in the *Gazette*, if the Agency has reasonable grounds to believe that such institution has successfully prevented the disruption or destruction of the computer system or computer program that would have serious impact on the national security, public health, public safety, confidentiality, or economic well being of citizens, or the effective functioning of the government or the economy of Sri Lanka.

**Obligations of  
the owner of the  
CII**

**18.** Upon the designation of an Institution having a computer system or computer program as CII, the owner of the CII shall -

- (a) be responsible for the protection of CII, in conformity with such requirements as may be prescribed.

Provided that, if the CII spreads across multiple institutions or multiple sectors, every owner of such institutions 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 against cyber threats or cyber security incidents subject to paragraph (a);

(ii) for assisting 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, by way of rules made 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 by way of rules made under this Act;

(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 by way of rules made under this Act; and

- (e) 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, manner and within a period of time as by way of rules made under this Act.

## **PART VI**

### **FUND OF THE AGENCY**

**Fund of the  
Agency**

**19.** (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; and

(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 and all such sums as are required to be paid out of the Fund.

## **PART VII**

### **PENALTIES**

Imposition of penalties to enforce compliance

**20.** (1) A person required to conform to the requirements in Part V of this Act and such other requirements as may be prescribed, who fails to so conform, shall in the first instance be provided a warning in writing by the Agency, and given specified period of time to conform to such requirements or show cause as to why such requirements are not fulfilled.

(2) In the event any person fails to conform to the written warning given under subsection (1) shall be liable to a penalty as may be prescribed, taking into consideration the nature and gravity of relevant non-compliance :

Provided however, such penalty shall not exceed a sum of rupees one million in any given case. Where a person who has been subjected to a penalty on a previous occasion, subsequently fails to conform to a requirement on any further occasion such person shall be liable to the payment of an additional penalty in a sum consisting of double the amount imposed as a penalty on the first occasion and for each non compliance after such first occasion.

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

(4) If a person who becomes liable to a penalty in terms of subsection (2) fails to pay such penalty, the Agency may make an ex- parte application to the Magistrate Court of Colombo for an Order requiring the payment of the penalty and upon such order being made such amount shall be recoverable in the same manner as a fine imposed by Court.

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

(6) 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 a 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.

(7) Without prejudice to the provisions of subsection (1) and (2), the Agency may issue a directive to any Institution that has without reasonable cause failed to comply in whole or in part with any obligations in Parts V of this Act.

(8) Where an Institution fails to comply with a directive issued under subsection (7), the Agency may, upon application to the High Court of the Western Province, holden in Colombo and upon satisfying the Court that an 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 the 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.

## **PART VIII**

### **MISCELLANEOUS**

**Financial year  
and audit of  
accounts**

**21.** (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 shall apply to the audit of the accounts of the Agency.

**Power of entry,  
inspection and  
search**

**22.** (1) The Agency or any other officer authorized in writing in that behalf by the Agency, may where it considers necessary for the purpose of discharging functions of the Agency, and ascertaining whether the provisions of this Act or any regulation made thereunder are being complied with under the authority of a warrant issued in that behalf by a Magistrate on application made on such purpose -

- (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.

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

(a) the investigation needs to be conducted urgently since it 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) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible.

(3) As soon as may be practicable the Agency shall and in any event within seventy two hours of such action make an application to the Magistrate to have the such action confirmed.

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

**23.** For the purpose of this Act –

- (a) the Agency; and
- (b) the CERT,

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**

**24.** 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,



**servants** 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** 25. (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** 26. (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** 27. (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**

**28.** (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.

**Duty to  
maintain  
confidentiality**

**29.** The Agency, CERT or any other institution, entity or person who obtain 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 reveal any information which may come to his knowledge in the performance or discharge of his duties or 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**

**30.** (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.

(3) Every rule published in the *Gazette* shall, within a period of three months of its publication in the *Gazette*, be brought before the Parliament for the approval.

#### **Regulations**

**31.** (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 CIIs;

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

- (c) the standards and procedures based on the cyber security policy to be adhered by the government and protection plans for computer programme or computer systems by government institutions;
- (d) the standards for accrediting the cyber security training program and training institutes;
- (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 the CIIs;
- (i) form and manner of reporting cyber security incidents and cyber threats 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) 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**

**32.** 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 program, performs automatic processing of data;

“computer programme” means a set of instructions that can be 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 under Article 43 or 44 of the Constitution;

“National Cyber Security Strategy” includes Cyber Security Strategies made from time to time approved by the Cabinet of Ministers;

“owner of the CII” means –

- (a) the head of a government department or institution, or a corporation established by or under any written law;
- (b) every director and other officer of a body corporate responsible for the CIIs;
- (c) every partner of a firm responsible for the CIIs ; or
- (d) every officer responsible for CIIs in an unincorporated body;

“prescribed” means prescribe by regulations under this Act.

**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.