Unofficial Translation*

CYBER SECURITY MAINTENANCE ACT, B.E. 2562 (2019)

HIS MAJESTY KING MAHA VAJIRALONGKORN PHRA VAJIRAKLAOCHAOYUHUA;

Given on the 24th Day of May B.E. 2562;

Being the 4th Year of the Present Reign.

His Majesty King Maha Vajiralongkorn Phra Vajiraklaochaoyuhua is graciously pleased to proclaim that:

Whereas it is expedient to have the law on cyber security maintenance;

Whereas this Act contains certain provisions in relation to the restriction of rights and liberties of persons, in respect of which section 26 in conjunction with section 28, section 32, section 33, section 34, section 36 and section 37 of the Constitution of the Kingdom of Thailand so permits by virtue of provisions of law;

Whereas the reasons and need for the restriction of rights and liberties of persons under this Act lie in putting forth efficiency of cyber security maintenance and putting forth measures for preventing, handling and reducing risks of cyber threats which affect national security and internal peace and order and, in this regard, the enactment of this Act duly complies with the conditions provided in section 26 of the Constitution of the Kingdom of Thailand;

Be it, therefore, enacted by the King, by and with the advice and consent of the National Legislative Assembly serving as the National Assembly, as follows.

---

* Translated by Associate Professor Dr. Pinai Nanakorn under contract for the Office of the Council of State of Thailand's Law for ASEAN project. – Tentative Version – subject to final authorisation by the Office of the Council of State.

Section 1. This Act is called the "Cyber Security Maintenance Act, B.E. 2562 (2019)".

Section 2.[1] This Act shall come into force as from the day following the date of its publication in the Government Gazette.

Section 3. In this Act:

"cyber security maintenance" means measures or operations established for preventing, handling and reducing risks of internal and external cyber threats affecting national security, economic security, military security and internal peace and order;

"cyber threat" means any unlawful act or operation which is performed by the use of a computer or a computer system or an undesirable programme with an intent to cause an act of violence against a computer system, computer data or other relevant data and which is an imminent danger causing damage to or affecting the functionality of a computer, a computer system or other relevant data;

"cyber" includes data and communications resulting from the provision of services, or the application of, a computer network, an internet system or a telecommunication network and also the regular provision of satellite services and similar networks of general connectivity;

"State agency" means central administration, provincial administration, local administration, a State enterprise, a legislative organ, a judicial organ, an independent organ, a public organisation and any other agency of the State;

"code of practice" means rules or directions prescribed by the Cyber Security Supervisory Committee;

"cyber security incident" means an incident resulting from any unlawful action or operation which is performed via a computer or a computer system and is likely to cause damage to or affect the cyber security maintenance or the cyber security of a computer, computer data, a computer system or other data relating to a computer system;

---

[1] Published in Government Gazette, Vol. 136, Part 69a, dated 27th May 2019.

"resolution measures for the cyber security maintenance" means the resolution of cyber security problems by the deployment of personnel, procedures and technology via a computer, a computer system, a computer programme or a service relating to any computer with a view to creating confidence in and strengthening the cyber security of a computer, computer data, a computer system or other data relating to a computer system;

"critical information infrastructure" means a computer or computer system which is used by a State agency or a private agency in its affairs in connection with the maintenance of national security, public safety, national economic security or infrastructure of public interests;

"critical information infrastructure agency" means a State agency or private agency which assumes missions or provides services in relation to critical information infrastructure**;**

"regulatory or supervisory agency" means a State agency, private agency or person that is designated by law to have duties and powers to regulate or supervise the operation of affairs of State agencies or critical information infrastructure agencies;

"Committee" means the National Cyber Security Committee;

"competent official" means the person appointed by the Minister for performing activities under this Act;

Secretary-General" means the Secretary-General of the National Cyber Security Committee;

"Office" means the Office of the National Cyber Security Committee;

"Minister" means the Minister having charge and control of the execution of this Act.

Section 4. The Prime Minister shall have charge and control of the execution of this Act and shall have the powers to issue Notifications and appoint competent officials in the execution of this Act.

Such Notifications shall come into force upon their publication in the Government Gazette.

CHAPTER I
COMMITTEES

PART I
NATIONAL CYBER SECURITY COMMITTEE

Section 5. There shall be a committee called the "National Cyber Security Committee" called "NCSC" in brief and called in the English language as the "National Cyber Security Committee" as abbreviated as "NCSC", consisting of:

(1) the Prime Minister as Chairperson;

(2) *ex officio* members, viz, the Minister of Defence, Minister of Digital Economy and Society, Permanent Secretary for Finance, Permanent Secretary for Justice, Commissioner-General of the Royal Thai Police and Secretary-General of the National Security Council;

(3) not more than seven qualified members appointed by the Council of Ministers from persons possessing apparent knowledge, expertise and experience in the cyber security maintenance, information and communication technology, personal data protection, science, engineering, law, finance or other areas relevant and beneficial to the cyber security maintenance.

The Secretary-General shall be a member and secretary and the Secretary-General shall appoint not more than two officials of the Office as assistant secretaries.

The rules and procedures for the selection of persons to be nominated to the Council of Ministers for being appointed as qualified members and the selection of qualified members to replace those who vacate office before the expiration of the term under section 7 paragraph two shall be in accordance with the Rule prescribed by the Council of Ministers upon recommendation by the Committee.

Section 6. A qualified member of the Committee shall be of Thai nationality and shall not be under the prohibitions as follows:

(1) being a bankrupt or having previously been a dishonest bankrupt;

(2) being an incompetent person or a *quasi*-incompetent person;

(3) having been sentenced to imprisonment by a final judgment of the Court, whether having been actually imprisoned or not, except for an offence committed through negligence or a petty offence;

(4) having previously been expelled or dismissed from or ordered to leave the Government service or an agency of his service by reason of any corruption in office or grave misconduct;

(5) having previously been removed from office established by law;

(6) being a holder of a political position, a member of a local assembly or a local administrator, an executive member or holder of a position responsible for the administration of a political party, an adviser to a political party or an official of a political party.

Section 7. A qualified member of the Committee shall hold office for a term of four years and may be re-appointed but may not serve for more than two consecutive terms.

In the case of an appointment of a qualified member as an additional one or as the one in replacement of a qualified member who vacates office before the expiration of the term, the person so appointed as an additional or replacing qualified member shall hold office for the remaining tern of the qualified members already appointed, except that in the case where there remain less than ninety days in the term of office the appointment of a replacing qualified member may be omitted.

At the expiration of the term under paragraph one, if new qualified members have not yet been appointed, the qualified members who vacate office at the expiration of such term shall remain in office for continuance of performance until new qualified members are appointed.

Section 8. In addition to the vacation of office upon the expiration of the term under section 7, a qualified member vacates office upon:

(1) death;

(2) resignation;

(3) being removed by the Council of Ministers;

(4) being disqualified or being under any prohibition under section 6.

Section 9. The Committee has the duties and powers as follows:

(1) to submit to the Council of Ministers, for approval, the policy and plan on the cyber security maintenance as well as the promotion and support of operations for the cyber security maintenance under section 42 and section 43, along the line of the directions laid down under section 42;

(2) to lay down the policy on the management in connection with the cyber security maintenance for State agencies and critical information infrastructure agencies;

(3) to prepare, for submission to the Council of Ministers, an action plan on the cyber security maintenance which shall serve as a master plan on the cyber security maintenance in a normal situation and in a situation where a cyber threat might occur or has occurred, provided that such plan shall be in line with national policies, strategies and plans as well as the framework policies and masterplans in connection with the security maintenance prepared by the National Security Council;

(4) to prescribe standards and directions for promoting and developing systems for the provision of services in connection with the cyber security maintenance, establish standards in connection with the cyber security maintenance and prescribe minimum standards relating to computers, computer systems and computer programmes and also promote accreditation of cyber security maintenance standards for critical information infrastructure agencies, State agencies, regulatory or supervisory agencies and private agencies;

(5) to prescribe measures and directions for elevating skills, knowledge and expertise, in the cyber security maintenance, of competent officials or officials of critical information infrastructure agencies, State agencies, regulatory or supervisory agencies and private agencies which are involved in the cyber security maintenance;

(6) to set a framework for co-ordinating co-operation with other domestic and foreign agencies which are involved in the cyber security maintenance;

(7) to appoint and remove the Secretary-General;

(8) to entrust the regulation and supervision to regulatory or supervisory agencies, State agencies or critical information infrastructure agencies and also lay down for

them requirements, objects, duties and powers and a framework for the operations in the cyber security maintenance;

(9) to monitor and assess the implementation of the policy and plan on the cyber security maintenance, action plan on the cyber security maintenance and operations for the cyber security maintenance as provided in this Act;

(10) to make recommendations and give advice, to the National Commission on Digitality for Economy and Society or the Council of Ministers, on matters in connection with the cyber security maintenance;

(11) to recommend to the Council of Ministers the enactment or revision of laws relating to the cyber security maintenance;

(12) to prepare a report providing a summary of operations involving the cyber security maintenance producing significant impacts or directions for developing cyber security maintenance standards, for submission to the Council of Ministers for information;

(13) to perform any other activities as provided in this Act or as entrusted by the Council of Ministers.

Section 10. Meetings of the Committee shall be in accordance with the Rule prescribed by the Committee. In this regard, meetings may be held by an electronic means or any other means.

Section 11. The Chairperson and members of the Committee shall receive meeting allowances or other remuneration in accordance with the rules prescribed by the Council of Ministers.

PART II
CYBER SECURITY SUPERVISORY COMMITTEE

Section 12. In the execution of duties and powers of the Committee under section 9, there shall be the Cyber Security Supervisory Committee called "CSSC" in brief, consisting of:

(1) the Minister of Digital Economy and Society as Chairperson;

(2) *ex officio* members, viz, the Permanent Secretary for Foreign Affairs, Permanent Secretary for Transport, Permanent Secretary for Digital Economy and Society, Permanent Secretary for Energy, Permanent Secretary for Interior, Permanent Secretary for Public Health, Commissioner-General of the Royal Thai Police, Supreme Commander-in-Chief, Secretary-General of the National Security Council, Director of the National Intelligence Agency, Governor of the Bank of Thailand, Secretary-General of the Office of the Securities and Exchange Commission and Secretary-General of the National Broadcasting and Telecommunications Commission;

(3) not more than four qualified members appointed by the Committee from persons possessing apparent knowledge, expertise and experience beneficial to the cyber security maintenance.

The Secretary-General shall be a member and secretary and the Secretary-General shall appoint not more than two officials of the Office as assistant secretaries.

The rules and procedures for the selection of persons deemed appropriate for being appointed as qualified members shall be in accordance with the Rule prescribed by the Committee.

Section 13. The CSSC has the duties and powers as follows:

(1) to monitor operations in the implementation of the policy and plan under section 9 (1) and section 42;

(2) to oversee and take action for handling critical cyber threats under section 61, section 62, section 63, section 64, section 65 and section 66;

(3) to supervise the operation of the National Centre for Co-ordination of the Computer System Security Maintenance and the incident action as well as computer forensic science;

(4) to prescribe a code of practice and a framework standard for the cyber security maintenance, thereby constituting minimum requirements for cyber security maintenance operations to be observed by State agencies and critical information infrastructure agencies and also lay down measures for assessing risks and reacting to as well as handling cyber threats upon their occurrence or upon incidents affecting or possibly affecting or causing

significant or serious damage to information systems of the country, with a view to facilitating fast, efficient and uniform operations in conducting the cyber security maintenance;

(5) to determine duties of critical information infrastructure agencies and duties of regulator or supervisory agencies, provided that regulator or supervisory agencies shall at least be required to have the duty to set appropriate standards for handling cyber threats of each critical information infrastructure agency and State agency;

(6) to determine levels of cyber threats as well as details of measures for preventing, handling, assessing, suppressing and terminating cyber threats of each level, for submission to the Committee;

(7) to analyse situations and assess impacts of cyber threats for submission to the Committee for consideration and giving directions when a cyber threat of a more severe level occurs or is expected to occur.

In prescribing the framework standard under paragraph one (4), regard shall be had to risk management principles, as to which the following methods and measures shall at least be an integral part thereof:

(1) the indication of possible risks to computers, computer data, computer systems, other data relating to computer systems and property, lives and physical conditions of persons;

(2) measures for preventing possible risks;

(3) measures for inspection and surveillance of cyber threats;

(4) incident action measures upon discovery of cyber threats;

(5) measures for remedying, and carrying out rehabilitation from, damage resulting from cyber threats.

Section 14. In carrying out activities under section 13 paragraph one (2) in the interest of the timely handling of cyber threats, the CSSC may delegate its power to the Minister of Digital Economy and Society, Supreme Commander-in-Chief and other members designated by the CSSC for carrying out operations in such matters jointly and may also require regulatory or supervisory agencies and critical information infrastructure agencies that are under attack to join operations, co-ordination and support.

The performance under paragraph one shall be in accordance with the Rule prescribed by the CSSC.

Section 15. The provisions of section 6, section 7 and section 8 shall apply to qualified members of the CSSC *mutatis mutandis*.

Section 16. The CSSC shall have the power to appoint sub-committees for performing any particular activities as entrusted by the CSSC.

Section 17. Meetings of the CSSC and sub-committees shall be in accordance with the Rule prescribed by the CSSC. In this regard, meetings may be held by an electronic means or any other means.

Section 18. The Chairperson and members, the chairperson of a sub-committee and members of a sub-committee appointed by the CSSC shall receive meeting allowances or other remuneration in accordance with the rules prescribed by the Council of Ministers.

Section 19. In the performance of duties under this Act, competent officials shall show identification cards to persons concerned.

In appointing competent officials, the Minister shall appoint persons possessing knowledge and expertise in the cyber security maintenance as competent officials for performing any particular activities under this Act. In this regard, levels of knowledge and expertise in the cyber security maintenance of competent officials shall be as prescribed in the Notification of the Committee.

Identification cards of competent officials shall be in accordance with the form prescribed in the Notification of the CSSC.

CHAPTER II
OFFICE OF THE NATIONAL CYBER SECURITY COMMITTEE

Section 20. There shall be the Office of the National Cyber Security Committee as a State agency which is ascribed the status of a juristic person and is neither a Government

agency under the law on the administrative organisation of State affairs nor a State enterprise under the law on budgetary procedures or other laws.

Section 21. Affairs of the Office is not subject to the law on labour protection, the law on labour relations, the law on social security and the law on compensation but officials and employees of the Office shall receive not lower remunerative benefits than those provided in the law on labour protection, the law on social security and the law on compensation.

Section 22. The Office shall be responsible for clerical work, technical work, meeting work and secretarial work of the Committee and the CSSC and shall also have the duties and powers as follows:

(1) to make recommendations and lend support to the Committee in relation to the preparation of the policy and plan on the cyber security maintenance and the action plan on the cyber security maintenance under section 9;

(2) to prepare the code of conduct and framework standard for the cyber security maintenance under section 13 paragraph one (4) for submission to the CSSC for approval;

(3) to co-ordinate operations on the cyber security maintenance of critical information infrastructure agencies under section 53 and section 54;

(4) to undertake co-ordination and provide co-operation in regard to the establishment of centres for co-ordination of the computer system security maintenance domestically and overseas in relation cyber security incidents and lay down resolution measures for the cyber security maintenance;

(5) to take action and co-ordinate with State and private agencies in reacting to and handling cyber threats as entrusted by the Committee;

(6) to conduct surveillance of cyber threat risks, follow, analyse and process data on cyber threats and also give warnings of cyber threats;

(7) to work and co-ordinate with, and lend support as well as provide assistance to, agencies concerned in connection with the implementation of the policy and plan on the cyber security maintenance, the action plan on the cyber security maintenance and measures

for preventing, handling and reducing cyber threat risks or in accordance with orders of the Committee;

(8) to take action and provide co-operation or assistance in regard to the prevention, handling and reduction of cyber threat risks, in particular, cyber threats affecting or occurring to critical information infrastructure;

(9) to strengthen knowledge and understanding in relation to the cyber security maintenance and create common awareness of cyber threat situations, with a view to putting forth integrated and up-to-date operational actions;

(10) to serve as a focal point for gathering and analysing information on the cyber security maintenance of the country and also disseminate information relating to risks and incidents involving the cyber security maintenance to State agencies and private agencies;

(11) to serve as a focal point for co-ordinating co-operation amongst agencies which are concerned in the cyber security maintenance of domestic and foreign State agencies and private agencies;

(12) to enter into agreements and co-operation with domestic and foreign organisations or agencies in affairs concerning operations in pursuit of duties and powers of the Office upon approval by the Committee;

(13) to study and research into information necessary for the cyber security maintenance with a view to making recommendations on cyber security maintenance measures and provide regular training and practice on cyber threat handling to agencies concerned;

(14) to promote, support and take action in the dissemination of knowledge on the cyber security maintenance and also provide training for elevating skills and expertise in the performance of duties in connection with the cyber security maintenance;

(15) to report progress and situations in connection with the execution of this Act and also problems and obstacles to the Committee for consideration and action, in accordance with periods of time as specified by the Committee;

(16) to perform any other activities in connection with the cyber security maintenance of the country, as entrusted by the Committee or the Council of Ministers.

For the purpose of taking action in pursuit of the duties and powers under (6), the Office shall establish the National Centre for Co-ordination of the Computer System Security Maintenance as its internal body, with the duties and powers as prescribed by the Committee.

Section 23. In carrying out activities of the Office, the Office shall also have general duties and powers as follows in addition to the duties and powers as provided under section 22:

(1) to hold ownership, possessory rights and real rights;

(2) to establish rights or enter into juristic acts of all types with proprietary binding effects and also enter into any other juristic act for the purpose of the operation of affairs of the Office;

(3) to provide and grant funding for supporting the operation of affairs of the Office;

(4) to collect fees, contribution fees, remuneration or service charges for the operation of affairs, in accordance with the rules and rates prescribed by the Office with the approval of the EBO;

(5) to perform any other activities provided by law to be the duties and powers of the Office or as entrusted by the Committee or the EBO.

Section 24. The fund and property for the operation of affairs of the Office consist of:

(1) the inaugural fund allocated by the Government under section 81 paragraph one and the money as well as property transferred under section 82;

(2) the general subsidy annually allocated by the Government as appropriate;

(3) contributions from domestic and foreign State agencies or intergovernmental organisations;

(4) fees, contribution fees, remuneration, service charges or incomes resulting from the operation of affairs in pursuit of the duties and powers of the Office;

(5) fruits of the money or incomes from property of the Office.

The money and property of the Office under paragraph one shall be remitted as State revenues.

Section 25. There shall be, for the purpose of supervising general administration of the Office, the Executive Board of the Office of the National Cyber Security Committee called "EBO" in brief consisting of the Minister of Digital Economy and Society as Chairperson, Permanent Secretary for Digital Economy and Society, Comptroller-General, Secretary-General of the Civil Service Commission, Secretary-General of the Office of the Public Sector Development Commission and not more than six qualified members, as members.

The Secretary-General shall be a member and secretary and the Secretary-General shall appoint not more than two officials of the Office as assistant secretaries.

Qualified members under paragraph one shall be appointed by the Minister from persons possessing apparent knowledge, expertise and ability in the areas of cyber security maintenance, information and communication technology, economics, social sciences, law, business administration or other areas relevant and beneficial to the operation of work of the EBO, in accordance with the rules and procedures prescribed by the Committee.

The provisions of section 6 and section 8 shall apply to qualified members *mutatis mutandis*.

Section 26. A qualified member of the EBO shall hold office for a term of four years.

In the case of an appointment of a qualified member as an additional one or as the one in replacement of a qualified member who vacates office before the expiration of the term, the Minister may appoint an additional or replacing qualified member and the person so appointed as an additional or replacing qualified member shall hold office for the remaining tern of the qualified members already appointed.

At the expiration of the term under paragraph one, if new qualified members have not yet been appointed, the qualified members who vacate office at the expiration of such term shall remain in office for continuance of performance until new qualified members are appointed.

Section 27. The EBO shall have the duties and powers as follows:

(1) to set the administration policy and approve action plans of the Office;

(2) to make regulations on institutional organisation, finance, personnel administration, general administration, procurement, internal auditing and also aids and welfare of the Office;

(3) to approve the expenditure plan and annual appropriation of the Office;

(4) to supervise the administration and operation of affairs of the Office and the Secretary-General to ensure conformity with this Act and other relevant laws;

(5) to decide administrative orders of the Secretary-General insofar as they are concerned with the administration of affairs of the Office;

(6) to assess the operation of affairs of the Office and the performance of the Secretary-General;

(7) to perform other duties as provided by this Act or other laws to be the duties and powers of the EBO or as entrusted by the Committee or the Council of Ministers.

In the performance of affairs under paragraph one, the EBO may appoint a sub-committee for considering, recommending or taking any particular act as entrusted by the EBO. In this regard, the performance of work and meetings shall be in accordance with the rules and procedures prescribed by the EBO.

The EBO may appoint qualified persons who possess expertise in areas beneficial to the operation of work of the Office as advisers to the EBO, in accordance with the rules and procedures prescribed by the Committee.

Section 28. The chairperson and members and the chairperson and members of a sub-committee appointed by the EBO shall receive meeting allowances and other remuneration in accordance with the rules prescribed by the Committee.

Section 29. The Office shall have a Secretary-General, who shall be responsible for the performance of work of the Office and become the superior of officials and employees of the Office.

Section 30. The Secretary-General shall have the qualifications as follows:

(1) being of Thai nationality;

(2) being not lower than thirty-five years of age but not over sixty years of age;

(3) being a person possessing knowledge, ability and experience in the area relating to missions of the Office and the administration.

Section 31. A person of any of the following descriptions shall be prohibited from being the Secretary-General:

(1) being a bankrupt or having previously been a dishonest bankrupt;

(2) being an incompetent person or a *quasi*-incompetent person;

(3) having been sentenced to imprisonment by a final judgment, whether having been actually imprisoned or not, except for an offence committed through negligence or a petty offence

(4) being a Government official, official or employee of a Government agency or a State enterprise or any other agency of the State or of a local administration;

(5) being or having previously been a political official, a holder of a political position, a member of a local assembly or a local administrator, except where not less than one year has elapsed since the vacation of office;

(6) being or having previously been an executive member of, or holder of any other position in, a political party or an official of a political party, except where not less than one year has elapsed since the vacation of office;

(7) having previously been expelled or dismissed from or ordered to leave the Government service or an agency of his service by reason of corruption in office or grave misconduct or having previously been removed from office;

(8) having previously been removed by reason of failing the performance assessment under section 35 (5).

Section 32. The Committee shall determine the rate of a monthly salary and other remuneration of the Secretary-General in accordance with the rules prescribed by the Council of Ministers.

Section 33. The Secretary-General shall hold office for a term of four years.

The Secretary-General who vacates office at the expiration of the term may be re-appointed but may not serve for more than two terms.

Section 34. In each year, the performance of the Secretary-General shall be assessed, in accordance with periods of time and procedures prescribed by the Committee.

Section 35. In addition to the vacation of office upon the expiration of the term, the Secretary-General vacates office upon:

(1) death;

(2) resignation;

(3) being disqualified under section 30 or being under any prohibition under section 31;

(4) being removed upon a resolution by the Committee by reason of neglect or corruption in office or misbehaviour or incompetence;

(5) being removed by the Committee by reason of failing the performance assessment;

(6) the occurrence of the case specified in the contract of employment or the agreement between the Committee and the Secretary-General.

Section 36. The Secretary-General shall, under the supervision of the Committee, the CSSC and the EBO, carry out activities in pursuit of orders of the Committee, the CSSC and the EBO, within the duties and powers as follows:

(1) to administer affairs of the Office with a view to the achievement of missions of the Office and in accordance with the policy and plan on the cyber security maintenance, the action plan on the cyber security maintenance, policies of the Council of Ministers and the Committee and Regulations, policies, resolutions and Notifications of the EBO;

(2) to lay down Rules under policies of the Committee and the CSSC in a manner not contrary to or inconsistent with the law, resolutions of the Council of Ministers and Regulations, policies, resolutions and Notifications issued by the Committee and the CSSC;

(3) to be the superior of officials and employees of the Office and assess performance of officials and employees of the Office in accordance with the Regulations of the EBO and the Rules of the Office;

(4) to appoint Deputy Secretary-Generals or assistant Secretary-Generals with the approval of the Committee for assisting the performance of work of the Secretary-General as entrusted by the Secretary-General;

(5) to recruit and appoint officials and employees of the Office, increase, reduce or cut their salaries or wages, inflict disciplinary penalty upon them and also remove them from office, in accordance with the Regulations of the EBO and the Rules of the Office;

(6) to perform any other activities in accordance with the Regulations, policies, resolutions or Notifications issued by the EBO or the CSSC.

In affairs of the Office which concern third persons, the Secretary-General shall represent the Office within the scope of the appointment by the Committee.

The Secretary-General may delegate powers to any person attached to the Office for performing any particular act on the Secretary-General's behalf, in accordance with the Regulations issued by the EBO.

In the case where there is no Secretary-General or the Secretary-General is unable to perform duties, the Deputy Secretary-General of respective seniority shall act as the Secretary-General. If there is no Deputy Secretary-General or Deputy Secretary-Generals are unable to perform duties, the Committee shall appoint an appropriate person to act as the Secretary-General.

Section 37. Accounting of the Office shall be carried out in accordance with the form and rules prescribed by the EBO, having regard to international principles and accounting standards.

Section 38. The Office shall prepare financial statements and accounts and submit the same to the auditor within ninety days as from the end of the accounting year.

The State Audit Office or a chartered auditor approved by the State Audit Office shall be the auditor of the Office and assess the expenditure of money as well as the disposal of property of the Office every year and prepare an audit report for submission to the EBO for adoption.

Section 39. The Office shall prepare an annual report on its operations for submission to the Committee and the Minister within one hundred eighty days as from the end of the accounting year and disseminate the report to the public.

The annual report on operations under paragraph one shall indicate details of financial statements as commented on by the auditor and the works of the Office as well as the reporting of the assessment of the operations of the Office in the past year.

The assessment of the operations of the Office under paragraph two shall be carried out by a third person approved by the EBO.

Section 40. The Minister shall have the power to exercise general superintendence of affairs of the Office to ensure conformity with the duties and powers of the Office, laws, national strategies, policies and plans of the Government and resolutions of the Council of Ministers concerned. For this purpose, the Minister shall have the power to order the Secretary-General to provide explanations, give opinions or prepare a report for submission to the Minister and shall have the power to suspend acts of the Office which are contrary to the duties and powers of the Office, laws, national strategies, policies and plans of the Government or resolutions of the Council of Ministers concerned and order an investigation of facts relating to the operation of the Office.

CHAPTER III
CYBER SECURITY MAINTENANCE

PART I
POLICY AND PLANS

Section 41. The cyber security maintenance shall be conducted by having regard to the uniformity and integration of operations of State agencies and private agencies and shall be in line with the national policy and plan on the development of digitality for economy and society under the law on digital development for economy and society and the policy and masterplan relating to the maintenance of security prepared by the National Security Council.

Operations in relation to the cyber security maintenance shall be aimed at creating potential for the prevention, handling and reduction of cyber threat risks, in particular, the protection of critical information infrastructure of the country.

Section 42. The policy and plan on the cyber security maintenance shall at least contain goals and directions as follows:

(1) the integration of the management in relation to the cyber security maintenance of the country;

(2) the creation of measures and mechanisms for developing potential for the prevention, handling and reduction of cyber threat risks;

(3) the creation of measures for the protection of critical information infrastructure of the country;

(4) the co-ordination of co-operation between the public and private sectors and the co-ordination of international co-operation for the purpose of the cyber security maintenance;

(5) the research and development of technology and bodies of knowledge relating to the cyber security maintenance;

(6) the development of personnel and experts in the area of the cyber security maintenance in both public and private sectors;

(7) the creation of awareness and knowledge of the cyber security maintenance;

(8) the development of rules and laws for the purpose of the cyber security maintenance.

Section 43. The Committee shall prepare the policy and plan on the cyber security maintenance in accordance with the directions under section 42 for submission to the Council of Ministers for approval and for publication in the Government Gazette. Upon its publication, State agencies, regulatory or supervisory agencies and critical information infrastructure agencies as specified in the policy and plan on the cyber security maintenance shall take action in the implementation of such policy and plan.

In the preparation of the policy and plan under paragraph one, the Office shall hold the hearing of opinions or meetings jointly with State agencies, regulatory or supervisory agencies and critical information infrastructure agencies.

Section 44. State agencies, regulatory or supervisory agencies and critical information infrastructure agencies shall expeditiously prepare a code of practice and a framework standard for the cyber security maintenance of each agency in line with the policy and plan on the cyber security maintenance.

The code of practice for the cyber security maintenance under paragraph one shall at least consist of the following matters:

(1) the plan on the inspection and assessment of risks involving the cyber security maintenance by an assessor, an internal auditor or a third-person independent auditor at least once a year;

(2) the plan on the handling of cyber threats.

For the purpose of the preparation of the code of practice for the cyber security maintenance under paragraph one, the Office shall, with the approval of the Committee, prepare a code of practice and a framework standard in order to be relied on by State agencies, regulatory or supervisory agencies or critical information infrastructure agencies as guidance for preparing their own code of practice or to be adopted as their own code of practice, and in the case where such agencies have not yet had a code of practice or have a code of practice which is incomplete or inconsistent with the code of practice and framework standard, such code of practice and framework standard shall govern.

PART II
MANAGEMENT

Section 45. State agencies, regulatory or supervisory agencies and critical information infrastructure agencies have the duty to prevent, handle and reduce cyber threat risks in accordance with the code of practice and framework standard for the cyber security maintenance of each agency and shall also proceed in the implementation of the code of

practice and framework standard for the cyber security maintenance under section 13 paragraph one (4).

In the case where State agencies, regulatory or supervisory agencies or critical information infrastructure agencies are unable to take action or perform in accordance with paragraph one, the Office may render assistance with respect to personnel or technological matters to such agencies at their request.

Section 46. For the purpose of the cyber security maintenance, the State agencies, regulatory or supervisory agencies and critical information infrastructure agencies shall give the Office the notification of names of officials of executive levels and operational levels in the interest of the co-ordination in relation to the cyber security maintenance.

In the case of any change of officials under paragraph one, the State agencies, regulatory or supervisory agencies and critical information infrastructure agencies shall expeditiously notify it to the Office.

Section 47. In the case where the performance of duties under this Act requires knowledge and expertise, the Committee or the CSSC may entrust the Secretary-General to employ experts as may be appropriate to particular work.

Experts under paragraph one shall possess such appropriate qualifications or experience as prescribed in the Notification of the Committee.

The Secretary-General shall issue expert identification cards to persons appointed and such persons shall, in the performance of duties, show identification cards as experts and shall, upon termination of duties, expeditiously return the identification cards to the Office.

PART III
CRITICAL INFORMATION INFRASTRUCTURE

Section 48. Critical information infrastructure denotes activities central to national security, military security, economic security and internal peace and order and it is the duty of the Office to support and assist the prevention, handling and reduction of cyber threat risks, in particular, cyber threats affecting or occurring to critical information infrastructure.

Section 49. The Committee shall have the power to issue a Notification prescribing agencies which assume missions or provide services in the following areas as critical information infrastructure agencies:

(1) national security;

(2) essential public services;

(3) finance and banking;

(4) information technology and telecommunication;

(5) transport and logistics;

(6) energy and public utilities;

(7) public health;

(8) other areas as additionally prescribed in the Notification of the Committee.

The consideration and prescription, in the Notification, of missions or services under paragraph one shall be in accordance with the rules prescribed by the Committee and published in the Government Gazette. In this regard, the Committee shall, from time to time, consider and review the prescription, in the Notification, of such missions or services as may be appropriate.

Section 50. The Committee shall have the power to issue a Notification prescribing the nature, duties and responsibilities of centres for co-ordination of the computer system security maintenance for critical information infrastructure agencies under section 49 for carrying out co-ordination on, exercising surveillance of, handling and resolving cyber threats. In this regard, the Committee may require State agencies which have readiness or regulatory or supervisory agencies for such critical information infrastructure agencies to perform such duties for the critical information infrastructure agencies under section 49 in whole or in part.

The consideration and prescription, in the Notification, of missions or services of the agencies under paragraph one shall be in accordance with the rules prescribed by the Committee and published in the Government Gazette. In this regard, the Committee shall, from time to time, consider and review the prescription, in the Notification, of such missions or services as may be appropriate.

Section 51. In the case of doubt or a challenge as regards the nature of agencies assuming missions or providing services in the areas prescribed in the Notification under section 49 or section 50, the Committee shall give a final decision thereon.

Section 52. For the purposes of contacts and co-ordination, critical information infrastructure agencies shall notify names and contact information of owners and possessors of computers and computer system administrators to the Office, their regulatory or supervisory agencies and the agencies under section 50 within thirty days as from the date of the Notification of the Committee under section 49 paragraph two and section 50 paragraph two or as from the date of the decision of the Committee under section 51, as the case may be. In this regard, owners and possessors of computers and computer system administrators must at least be persons responsible for the administration of such critical information infrastructure agencies.

In the case of any change of owners and possessors of computers and computer system administrators under paragraph one, notification thereof shall be given to the agencies concerned under paragraph one not less than seven days prior to the change except that, in the case of inevitable necessity, the notification shall be given expeditiously.

Section 53. In carrying out the cyber security maintenance of critical information infrastructure agencies, regulatory or supervisory agencies shall inspect minimum standards as regards cyber security of critical information infrastructure agencies within their supervision. If it is found that any critical information infrastructure agency fails to meet the standard, such regulatory or supervisory agencies shall, without delay, notify the critical information infrastructure agency which fails to meet the standard to carry out rectification in order to meet the standard expeditiously. If such critical information infrastructure agency fails to take action or fails to accomplish the action within the period of time specified by the regulatory or supervisory agency, the regulatory or supervisory agency shall refer the matter to the CSSC for consideration without delay.

Upon receipt of a complaint under paragraph one, if the CSSC is of the opinion, after its consideration, that such incident occurs and may cause a cyber threat, the CSSC shall take action as follows:

(1) in the case of a State agency, notifying the matter to its chief executive officer for the purpose of exercising the administrative power in instructing such State agency or critical

information infrastructure agency to carry out the rectification towards the satisfaction of the standard expeditiously;

(2) in the case of a private agency, notifying the matter to its chief executive officer, possessors of computers and administrators of computer systems of such critical information infrastructure agency for the purpose of carrying out the rectification towards the satisfaction of the standard expeditiously.

The Secretary-General shall also carry out follow-ups to ensure the compliance with the provisions of paragraph two.

Section 54. A critical information infrastructure agency shall cause risks involving the cyber security maintenance to be assessed by an assessor and shall also put in place the auditing of cyber security by both internal and third-party independent auditors of information security at least once a year.

A critical information infrastructure agency shall furnish a summary of a report on the operations to the Office within thirty days as from the date of completion.

Section 55. In the case where the CSSC is of the opinion that the assessment of risks involving the cyber security maintenance or the auditing of cyber security under section 54 fails to meet the standard, as revealed by a report prepared by a regulatory or supervisory agency, the CSSC shall order such critical information infrastructure agency to carry out a risk assessment anew to ensure the satisfaction of the standard or carry out the auditing in other aspects which may affect critical information infrastructure.

In the case where such critical information infrastructure agency has already put in place the assessment of risks involving the cyber security maintenance or the auditing of cyber security under paragraph one but the CSSC is of the opinion that it remains unable to meet the standard, the CSSC shall take action as follows:

(1) in the case of a State agency, notifying the matter to its chief executive officer for the purpose of exercising the administrative power in instructing such State agency or critical information infrastructure agency to carry out the rectification towards the satisfaction of the standard expeditiously;

(2) in the case of a private agency, notifying the matter to its chief executive officer, possessors of computers and administrators of computer systems of such critical

information infrastructure agency for the purpose of carrying out the rectification towards the satisfaction of the standard expeditiously.

The Secretary-General shall also carry out follow-ups to ensure the compliance with the provisions of paragraph two.

Section 56. A critical information infrastructure agency shall put in place mechanisms or procedures for surveillance of cyber threats or cyber security incidents which are concerned with its critical information infrastructure in accordance with the standard prescribed by the regulatory or supervisory agency and in accordance with the code of practice as well as resolution measures for the cyber security maintenance as prescribed by the Committee or the CSSC and shall participate in a test of cyber threat handling readiness organised by the Office.

Section 57. Upon occurrence of a cyber threat which significantly affects a system of a critical information infrastructure agency, the critical information infrastructure agency shall report it to the Office and the regulatory or supervisory agency and carry out the handling of the cyber threat as provided in Part IV. In this regard, the CSSC may also prescribe rules and procedures for the reporting.

PART IV
CYBER THREAT HANDLING

Section 58. In the case where a cyber threat occurs or is expected to occur to an information system within the oversight and responsibility of any State agency or critical information infrastructure agency, such agency shall take action in inspecting its relevant data, computer data and computer systems and also surrounding circumstances for the purpose of assessing whether the cyber threat has actually occurred. If the inspection reveals that the cyber threat has occurred or is expected to occur, it shall take action for preventing, handling and reducing cyber threat risks in accordance with the code of practice and framework standard for the cyber security maintenance of such agency and notify the matter to the Office and its regulatory or supervisory agency expeditiously.

In the case where any agency or person encounters obstacles to or problems in the prevention, handling and reduction of its or his cyber threat risks, such agency or person may address a request to the Office for assistance.

Section 59. When it appears to a regulatory or supervisory agency or when a regulatory or supervisory agency has been notified of the incident under section 58, the regulatory or supervisory agency shall collaborate with agencies under section 50 in gathering data, examining and analysing situations and assess impacts in connection with cyber threats and take action as follows:

(1) lending support and rendering assistance to State agencies or critical information infrastructure agencies within its control or supervision and carrying out co-operation and co-ordination with the Office in the prevention, handling and reduction of cyber threat risks;

(2) expeditiously giving warnings to State agencies and critical information infrastructure agencies within its control or supervision as well as regulatory or supervisory agencies of other State agencies or critical information infrastructure agencies concerned.

Section 60. In its consideration for the purpose of exercising powers in the prevention of cyber threats, the Committee may prescribe the nature of cyber threats and classify them into three levels as follows:

(1) a non-serious cyber threat, which means a cyber threat posing a significant risk to the extent causing a computer system of a critical infrastructure agency of the country or the provision of public services to become less efficient;

(2) a serious cyber threat, which means a threat significantly increasing attacks against a computer system, computers or computer data with a view to attacking critical infrastructure of the country and thereby causing a computer system or critical information infrastructure pertinent to the provision of critical infrastructure services of the country, national security, international relations, national defence, economy, public health, public safety or public peace and order to be so injurious as to be incapable of functionality or out of service;

(3) a critical cyber threat, which means a critical cyber threat of the following descriptions:

(a) being a cyber threat resulting from an attack against a computer system, computers or computer data at a higher level than that of a serious cyber threat, in that it generates severe effects on critical information infrastructure of the country so comprehensively as to put the operation of State agencies or the provision of critical infrastructure services of the country to the public into total failure such that the State is unable to control central functionality of computer systems of the State or the employment of regular remedial measures for resolving the threat becomes unworkable, with the possibility that the threat spreads to other critical infrastructure of the country and thereby gives rise to fatality of a large number of people or destruction of a large number or amount of computer systems, computers or computer data to a comprehensive and nationwide extent;

(b) being a cyber threat which affects or possibly affects public peace and order or causes harm to national security or possibly causes the country or any part of the country to be in a state of emergency or face the commission of offences relating to terrorism under the Penal Code, a battle or a war such that urgent measures are needed for upholding the democratic regime of government with the King as Head of the State under the Constitution of the Kingdom of Thailand, the independence and territorial integrity, national benefits, the observance of laws, public safety, peaceful living of the people, the protection of rights and liberties, public peace and order or interests or the prevention or cure of damage from public disasters of an urgent and severe nature.

Details of the nature of cyber threats and measures for preventing, handling, assessing, suppressing and terminating cyber threats of each level shall be prescribed in the Notification of the Committee.

Section 61. When it appears to the CSSC that a serious cyber threat occurs or is expected to occur, the CSSC shall order the Office to take action as follows:

(1) gathering information and documentary evidence, witnesses or physical evidence concerned for the purposes of analysing situations and assessing impacts of the cyber threat;

(2) supporting, assisting and participating in the prevention, handling and reduction of emerging cyber threat risks;

(3) preventing cyber security incidents resulting from the cyber threat, recommending or ordering the use of resolution mechanisms for the cyber security maintenance and also finding directions for countering or resolving cyber security problems;

(4) encouraging the Office and agencies concerned, in public and private sectors, to assist and participate in the prevention, handling and reduction of emerging cyber threat risks;

(5) giving warnings of the cyber threat for information as is necessary and appropriate, having regard to the situation and the gravity as well as impacts of such cyber threat;

(6) facilitating the co-ordination amongst State agencies concerned as well as private agencies for managing risks and cyber security incidents.

Section 62. In the execution of section 61 for the purposes of analysing situations and assessing impacts of cyber threats, the Secretary-General shall order competent officials to take action as follows:

(1) making written requests for co-operation from persons concerned for the purpose of providing information within an appropriate period of time and at a specified place or providing, in writing, information on cyber threats;

(2) making written requests for information, documents or copies of information or documents which are in possession of other persons and beneficial to the conduct of operations;

(3) addressing questions to persons possessing knowledge and understanding of facts and situations connected with cyber threats;

(4) entering immovable property or places of business connected with or expectedly connected with cyber threats of persons or agencies concerned upon consent of the possessor of such place.

A person who provides information under paragraph one in good faith shall be afforded protection and shall not be deemed to commit a wrongful act or a breach of contract.

Section 63. In the case where it is necessary for the prevention, handling and reduction of cyber threat risks, the CSSC shall order State agencies to provide information and

lend support through the provision of their personnel or the use of electronic devices which are in their possession and related to the cyber security maintenance.

The CSSC shall exercise supervision to prevent the use of information acquired under paragraph one in a possibly injurious manner and the CSSC shall be responsible for remuneration of personnel and costs or damage from the use of such electronic devices.

The provisions of paragraph one and paragraph two shall also apply to requests to be addressed to private individuals with their consent.

Section 64. In the case where a serious cyber threat occurs or is expected to occur, the CSSC shall take action in preventing, handling and reducing cyber threat risks and pursue necessary measures.

In the execution of paragraph one, the CSSC shall instruct, in writing, State agencies concerned with the cyber security maintenance to perform or cease any action for the purposes of preventing, handling and reducing cyber threat risks in an appropriate and efficient manger in accordance with the directions determined by the CSSC and also undertake integrated collaboration in promptly controlling, terminating or mitigating consequences of such cyber threat.

The Secretary-General shall continually report the operations under this section to the CSSC and shall, when such cyber threat ceases to exist, expeditiously report results of the operations to the CSSC.

Section 65. In handing and mitigating damage from a serious cyber threat, the CSSC has the power to order, only to the extent necessary for preventing the cyber threat, owners, possessors or users of computers or computer systems or administrators of computer systems who are reasonably believed to be connected with the cyber threat or affected by the cyber threat to take action as follows:

(1) exercising surveillance of computers or computer systems in a particular period of time;

(2) inspecting computers or computer systems for finding defects which affect the cyber security maintenance, analysing situations and assessing impacts of the cyber threat;

(3) taking measures for resolving the cyber threat in order to cope with defects or eliminate undesirable instruction sets or terminate or mitigate the cyber threat in operation;

(4) retaining the status of computer data or computer systems by any means for the purpose of conducting operations in computer forensic science;

(5) gaining access to computer data or computer systems or other data relating to computer systems concerned only to the extent necessary for preventing the cyber threat.

In the case where there exists a need for gaining access to the data under (5), the CSSC shall entrust the Secretary-General to file a motion with the competent Court for ordering owners, possessors or users of computers or computer systems or administrators of computer systems under paragraph one to take action required by the motion. In this regard, a motion filed with the Court shall indicate a reasonable cause to believe that any particular person is committing or will be committing a particular act which gives rise to a serious cyber threat. In the consideration of a motion, a request shall be made for the conduct of an urgent inquiry into the motion and the Court shall expeditiously conduct the inquiry.

Section 66. In preventing, handling and reducing risks of serious cyber threats, the CSSC has the power to carry out or order competent officials to carry out operations, only to the extent necessary for preventing cyber threats, in the following matters:

(1) entering a place for inspection upon written notification of a reasonable cause to the owner or possessor of such place if there is a reasonable cause to believe that there are computers or computer systems which are connected to cyber threats or affected by cyber threats;

(2) gaining access to computer data, computer systems or other data relating to computer systems or making copies of or screening data or information or computer programmes reasonably believed to be connected with or affected by cyber threats;

(3) testing functionality of computers or computer systems reasonably believed to be connected with or affected by cyber threats or used for searching any data stored therein or utilised therefrom;

(4) seizing or attaching, only to the extent necessary, computers, computer systems or any equipment reasonably believed to be connected with cyber threats for inspection or analysis for a period not exceeding thirty days and, at the expiration of such

period, returning computers or any equipment to owners or possessors immediately after completion of the inspection or analysis.

In carrying out activities under (2), (3) and (4), the CSSC shall file a motion with the competent Court for ordering competent officials to take action indicated in the motion. In this regard, a motion shall indicate a reasonable cause to believe that any particular person is committing or will be committing a particular act which gives rise to a serious cyber threat. In the consideration of a motion, a request shall be made for the conduct of an urgent inquiry into the motion and the Court shall expeditiously conduct the inquiry.

Section 67. In the case where there occurs a critical cyber threat, it shall be the duty and power of the National Security Council to carry out the cyber security maintenance under the law on the National Security Council and other relevant laws.

Section 68. In the case where the incident is a matter of emergency and the treat in question is a critical cyber threat, the Committee may entrust the Secretary-General to take immediate action to the extent necessary for preventing and remedying damage in advance without filing a motion with the Court, provided that after having taken such action details thereof shall expeditiously be given to the competent Court.

In the case of an incident of serious or critical nature, for the purposes of preventing, assessing, handling, suppressing, terminating and reducing cyber threat risks, the Secretary-General shall, with the approval of the Committee or the CSSC, have the power to request up-to-date and consistent information from persons connected with cyber threats. In this instance, such persons shall expeditiously give the Committee or the CSSC co-operation and assistance.

Section 69. A person to whom an order in connection with the handling of a cyber threat is given may appeal against the order only if the cyber threat in question is a non-serious one.

CHAPTER IV
PENALTIES

———————

Section 70. A competent official under this Act shall not disclose or furnish computer data, log files, other data relating to computer systems or data of providers which are acquired under this Act to any person. Any person who violates this prohibition shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

The provisions of paragraph one shall not apply to action performed for the purpose of taking legal proceedings against offenders under this Act or offenders under other laws or for the purpose of taking legal proceedings against competent officials in connection with the unlawful exercise of powers and duties.

Section 71. Any competent official under this Act who negligently causes any other person to gain the knowledge of computer data, log files, data of providers or other data relating to computer systems which have been acquired under this Act shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.

Section 72. Any person who, having gained the knowledge of computer data, log files, data of providers or other data relating to computer systems acquired by a competent official under this Act, unlawfully discloses such data to any person shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both.

Section 73. Any critical information infrastructure agency which fails to report cyber threats under section 57 without any reasonable cause shall be liable to a fine not exceeding two hundred thousand Baht.

Section 74. Any person who fails to comply with a written request made by a competent official or fails to furnish information to a competent official under section 62 (1) or (2) without any reasonable cause, as the case may be, shall be liable to a fine not exceeding one hundred thousand Baht.

Section 75. Any person who violates or fails to comply with an order of the CSSC under section 65 (1) and (2) without any reasonable cause shall be liable to a fine not exceeding three hundred thousand Baht and an additional fine not exceeding ten thousand

Baht a day as from the expiration of the period of time specified by the order issued by the CSSC until correct action is performed.

Any person who violates or fails to comply with an order of the CSSC under section 65 (3) and (4) or fails to comply with an order of the Court under section 65 (5) shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.

Section 76. Any person who obstructs or fails to comply with an order of the CSSC or a competent official who takes action in pursuit of an order of the CSSC under section 66 (1) or fails to comply with an order of the Court under section 66 (2), (3) or (4) without any reasonable cause shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.

Section 77. In the case where the offender under this Act is a juristic person, if the commission of the offence by such juristic person has resulted from the instruction or an action of a director or a manager or any person responsible for the operation of such juristic person or in the case where such person has the duty to give instructions or take action and refrains from giving instructions or taking action, thereby leading to the commission of the offence by such juristic person, such person shall also be liable to the penalty as provided for such offence.

TRANSITORY PROVISIONS

Section 78. In the initial period, the Committee shall consist of the Chairperson and members under section 5 (1) and (2) and the Secretary-General of the National Cyber Security Committee shall be a member and secretary for performing duties to the extent necessary for the time being, and action shall be taken for completing the appointment of qualified members of the Committee under section 5 (3) within ninety days as from the date on which this Act comes into force.

In appointing qualified members under paragraph one, the Minister of Digital Economy and Society may also nominate persons to the Council of Ministers for considering and appointing as such qualified members.

Section 79. Action shall be taken in order to have the CSSC and the EBO within ninety days as from the date of the appointment of qualified members of the Committee under section 78.

Action shall be taken for completing the appointment of the Secretary-General of the National Cyber Security Committee under this Act within ninety days as from the date of the completion of the establishment of the Office under section 80.

Section 80. Action shall be taken for completing the establishment of the Office for performing operations under this Act within one year as from the date on which this Act comes into force.

Pending the completion of the establishment of the Office, the Office of the Permanent Secretary for Digital Economy and Society shall serve as the Office under this Act and the Permanent Secretary for Digital Economy and Society shall serve as Secretary-General until the appointment of the Secretary-General is made under section 79 paragraph two.

Section 81. In the initial period, the Council of Ministers shall allocate an inaugural fund to the Office as is necessary.

The Minister shall propose to the Council of Ministers for instructing Government officials, employees, officials or any other workers in State agencies to perform duties at the Office for the time being within a period of time specified by the Council of Ministers.

It shall be deemed that Government officials, employees, officials or any other workers in State agencies who perform duties at the Office for the time being under paragraph two retain their original status and remain entitled to salaries or wages, as the case may be, from their original agencies. In this regard, the Committee may also determine special remuneration for Government officials, employees, officials or any other workers in State agencies under paragraph two during their performance of duties at the Office.

Within one hundred eighty days as from the completion of the establishment of the Office, the Office shall take action in selecting Government officials, employees, officials or any other workers in State agencies under paragraph two for the purpose of recruiting them as employees of the Office.

Any Government official, employee, official or other worker in a State agency who is selected and recruited under paragraph four shall be entitled to count a period of previous service at the original agency into a period of service at the Office under this Act on a continual basis.

Section 82. When this Act comes into force, the Minister shall propose to the Council of Ministers for approving a transfer of all powers, duties, undertakings, property, rights, liabilities and budgets of all missions relating to the cyber security maintenance of the Office of the Permanent Secretary of the Ministry of Digital Economy and Society and the Electronic Transactions Development Agency as in existence on the day prior to the date on which this Act comes into force to the Office under this Act.

Section 83. The issuance of Ministerial Regulations, Rules and Notifications under this Act shall be completed within one year as from the date on which this Act comes into force. If their completion cannot be achieved, the Minister shall report the reasons therefor to the Council of Ministers for information.

Countersigned by:

General Prayut Chan-o-cha
Prime Minister