(Unofficial Translation)

No. 136 Chapter 69 Kor Government Gazette 27 May 2019

[Official Emblem of Royal Command]

Cybersecurity Act, B.E. 2562 (2019)

His Majesty King Phra Poramenthra Ramathibodi Sisin Maha Vajiralongkorn Phra Vajira Klao Chao Yu Hua

Given on the 24th Day of May B.E. 2562;
Being the 4th Year of the Present Reign.

His Majesty King Phra Poramenthra Ramathibodi Sisin Maha Vajiralongkorn Phra Vajira Klao Chao Yu Hua is graciously pleased to proclaim that:

Whereas it is expedient to have an enabling act on the law concerning maintaining cybersecurity.

This Act contains certain provisions in relation to the restriction of rights and freedom of a person, 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 permit by virtue of the law.

The rationale and necessity to restrict the rights and freedom of a person in accordance with this Act are to efficiently protect cybersecurity and to establish approaches to protect, cope with, and mitigate the risk of Cyber Threats which affect the national security and public order. The enactment of this Act is consistent with the criteria prescribed under 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 acting as the parliament, as follows:

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

Section 2 This Act shall come into force on the day following the date of its publication in the *Government Gazette*.

Section 3 Under this Act,

"Maintaining Cybersecurity" shall mean any measure or procedure established to prevent, cope with, and mitigate the risk of Cyber Threats from both inside and outside the country which affect national security, economic security, martial security, and public order in the country;

"Cyber Threats" shall mean any action or unlawful undertaking by using the computer, computer system, or undesirable program with an intention to cause any harm to the computer system, computer data, or other relevant data, and be an imminent threat to damage or affect operation of the computer, computer system, or other relevant data;

“Cyber” shall include data and communication from the service providing or application of the computer networks, internet system, or telecommunication networks including the usual service provision of satellite and other similar network systems which are generally connected;

"Government Agency" shall mean the central government, regional government, local

government, state enterprises, the legislative institution, the judicial institution, independent institutions, public agency, and other government agencies;

"Code of Practice" shall mean any regulations or rules determined by the Cybersecurity Regulating Committee;

"Cybersecurity Incident" shall mean an incident caused by any action or unlawful undertaking committed through a computer or computer system which may damage or affect Cybersecurity or cybersecurity of a computer, computer data, computer system, or other data related to the computer system;

"Cybersecurity Solution" shall mean the act of solving a cybersecurity issue by using personnel, process, and technology through a computer, computer system, computer program, or any service related to a computer, to create confidence and enhance cybersecurity of the computer, computer data, computer system, or other data related to the computer system;

"Critical Information Infrastructure" shall mean the computer or computer system that the Government Agency or private organization uses in their operations which relate to maintaining national security, public security, national economic security, or infrastructures in the public interest;

"Organization of Critical Information Infrastructure" shall mean a Government Agency or private organization who has a mission of or provides a Critical Information Infrastructure service;

"Supervising or Regulating Organization" shall mean a Government Agency or private organization or a person that is appointed by law to have the duty and power to supervise or regulate the operations of a Government Agency or Organization of Critical Information Infrastructure;

"Committee" shall mean the National Cybersecurity Committee;

"Competent Official" shall mean a person appointed by the Minister for the execution of this Act;

"Secretary-General" shall mean the secretary-general of the National Cybersecurity Committee;

"Office" shall mean the Office of the National Cybersecurity Committee;

"Minister" shall mean the Minister who is in charge of this Act.

Section 4 The Prime Minister shall be in charge of this Act and shall have the power to issue notifications related hereto and appoint the Competent Official for execution of this Act.

Notifications, shall come into force upon its publication in the *Government Gazette.*

Chapter 1
Committee

Part 1
National Cybersecurity Committee

Section 5 There shall be a committee named the "National Cyber Security Committee". The English name shall be "National Cyber Security Committee" abbreviated as "NCSC." The NCSC shall be comprised of:

(1) the Prime Minister as a chairperson;

(2) directors by position, comprising the Minister of Defence, Minister of Digital Economy and Society, Permanent Secretary of the Ministry of Finance, Permanent Secretary of the Ministry of Justice, , Commissioner-General of the National Police

Bureau, and Secretary-General of the National Security Council;

(3) honorary directors not exceeding seven persons, appointed by the Cabinet, who have knowledge, expertise, and remarkable experience in Maintaining Cybersecurity, information technology and communications, protection of data privacy, science, engineering, law, finance, or other relevant aspects which are beneficial to Maintaining Cybersecurity.

The Secretary-General shall be a director and secretary, and the Secretary-General shall appoint assistant secretaries from the officials of the Office not exceeding two persons.

The criteria and selection methods for the persons to be proposed to the Cabinet as honorary directors, including the selection of honorary directors to stay in the office in replacement of a person who vacated the office prior to the expiry of the term in accordance with section 7 paragraph two shall be in accordance with the rules as determined by the Cabinet as suggested by the Committee.

Section 6 Honorary directors in the Committee must have Thai nationality and shall not possess the following prohibited characteristics:

(1) being bankrupt or having been previously dishonestly bankrupt;

(2) be an incompetent or quasi-incompetent person;

(3) having been previously imprisoned by final court judgement, regardless of whether there was actual punishment of imprisonment, except for offenses committed by negligence or misdemeanors;

(4) having been previously dismissed, fired, or removed from an official position or any other previous organization on grounds of dishonest performance of duties or severe wrongful conduct;

(5) having been previously removed from an official position by way of the law;

(6) be a person holding a political position or serving as a local councilor, local administer, or director of, or a person responsible for managing a political party, counsel of a political party, or an officer of a political party.

Section 7 An honorary director in the Committee shall have a four-year term for each office, and may be reappointed, but shall not be in the office for more than two consecutive terms.

In case of the additional appointment of the honorary director or the replacement of the honorary director who has vacated the office prior to the expired term, the honorary director who has been additionally appointed or appointed in replacement of the vacant office shall stay in the office for the remaining period of the term of the appointed honorary director, unless the remaining term is less than ninety days, the honorary director may not be appointed.

When the term expires in accordance with paragraph one, if the new honorary director has yet to be appointed, the honorary director whose term has expired shall remain in the office to further perform the duties until a new honorary director is appointed.

Section 8 Apart from the expiration of term under section 7, an honorary director vacates office upon:

(1) death;

(2) resignation;

(3) being dismissed by an order of the Cabinet;

(4) lacking qualifications or possessing the prohibited characteristics as specified in section 6.

Section 9 The Committee shall have the following duties and powers to:

(1) propose the policy and plan on Maintaining Cybersecurity, promote, and support the act of Maintaining Cybersecurity in accordance with section 42 and section 43 for the Cabinet's approval, which shall be in accordance with the guideline specified under section 42;

(2) determine management policy for Maintaining Cybersecurity for the Government Agency and Organization of Critical Information Infrastructure;

(3) prepare the operational plan for Maintaining Cybersecurity to propose to the Cabinet as a master plan for Maintaining Cybersecurity under general situations and situations where the Cyber Threats may occur or have occurred; such plan shall be in accordance with the policy, strategy, and national plan as well as the policy framework and master plan which are related to maintaining the security of the National Security Council;

(4) establish the standard and guideline to enhance and develop service systems pertaining to Maintaining Cybersecurity, establish the standard in respect of Maintaining Cybersecurity, and determine the minimum standard pertaining to a computer, computer system, computer program, as well as support the certifying of standards for Maintaining Cybersecurity of Organization of Critical Information Infrastructure, Government Agency, Supervising or Regulating Organization, and private organizations;

(5) prescribe measures and guidelines to enhance the knowledge and expertise in Maintaining Cybersecurity of the Competent Officials, officers of the Organization of Critical Information Infrastructure, Government Agency, Supervising or Regulating Organization, and private organizations which are related to Maintaining Cybersecurity;

(6) set out a framework on coordinating with other agencies, both in the country and foreign countries, which are related to Maintaining Cybersecurity;

(7) appoint and remove the Secretary-General;

(8) assign the supervision and regulation, including the issuing of regulations, objectives, duties and power, and the operational framework regarding Maintaining Cybersecurity to the Supervising or Regulating Organization, Government Agency, or the Organization of Critical Information Infrastructure.

(9) monitor and evaluate the results of operating in accordance with the policy and plan on Maintaining Cybersecurity, operational plan for Maintaining Cybersecurity, and of Maintaining Cybersecurity as specified under this Act;

(10) suggest and provide opinions to the Digital Economy and Society Committee or to the Cabinet on Maintaining Cybersecurity;

(11) suggest to the Cabinet the legislation or amendment of laws related to Maintaining Cybersecurity;

(12) prepare a summary report of undertakings of Maintaining Cybersecurity that have significant effect, or the approach for developing the standard of Maintaining Cybersecurity for the Cabinet to be informed;

(13) perform any other task as specified under this Act or as assigned by the Cabinet.

Section 10 The meeting of the Committee shall be in accordance with the rules as determined by the Committee, where the meeting may proceed via electronic means or other means.

Section 11 The chairperson and the directors shall receive a meeting allowance or

other compensation in accordance with the rules determined by the Cabinet.

Part 2
Cybersecurity Regulating Committee

Section 12 In undertaking the duty and power of the Committee in accordance with section 9, there shall be a Cybersecurity Regulating Committee abbreviated as "CRC," comprising:

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

(2) directors by position, comprising the Permanent Secretary of the Ministry of Foreign Affairs, Permanent Secretary of the Ministry of Transport, Permanent Secretary of the Ministry of Digital Economy and Society, Permanent Secretary of the Ministry of Energy, Permanent Secretary of the Ministry of Interior, Permanent Secretary of the Ministry of Public Health, Commissioner-General of the National Police Bureau, Supreme Commander, Secretary-General of the National Security Council, Director of the National Intelligence Agency, Governor of the Bank of Thailand, Secretary-General of the Securities and Exchange Commission, and the Secretary-General of the National Broadcasting and Telecommunications Commission;

(3) honorary directors not exceeding four persons, who are appointed by the Committee among the persons who have knowledge, expertise, and experience which is remarkable and beneficial to Maintaining Cybersecurity.

The Secretary-General shall be a director and secretary, and the Secretary-General shall appoint assistant secretaries from the officials of the Office not exceeding two persons.

The criteria and selection methods for the appropriate persons to appoint as honorary directors shall comply with the rules as determined by the Committee.

Section 13 The CRC shall have the following duties and powers:

(1) monitor the undertaking in accordance with the policy and plan according to section 9 (1) and section 42;

(2) monitor and undertake in order to cope with Cyber Threats at critical level in accordance with section 61, section 62, section 63, section 64, section 65, and section 66;

(3) regulate the undertaking of the national coordinating agencies for the security of computer systems and the incident response and computer forensic science;

(4) determine the Code of Practice and standard framework in Maintaining Cybersecurity which are the minimum requirement in the act of Maintaining Cybersecurity for the Government Agency and the Organization of Critical Information Infrastructure, including determining the measure for risk assessment of, responses to, and coping with the Cyber Threats when there are any Cyber Threats or incidents that affect or may significantly or severely affect or damage the information system of the country for the quick, efficient, and united act of Maintaining Cybersecurity;

(5) determine the duties of Organization of Critical Information Infrastructure and duties of the Supervising or Regulating Organization which should at least determine the duties for the Supervising or Regulating Organization to determine the appropriate standards for each Organization of Critical Information Infrastructure and Government Agency in coping with Cyber Threats;

(6) prescribe the level of Cyber Threats including the details of the measures to

prevent, cope with, assess, suppress, and suspend the Cyber Threats at each level to present to the Committee;

(7) analyze the situation and evaluate the effect from Cyber Threats, in order to propose to the Committee to consider issuing an order, in the case there is or may be an occurrence of a Cyber Threat in a level that is more critical.

In determining the standard framework according to paragraph one (4), the risk management principals shall be considered, which shall contain at least the approaches and measures as follows;

(1) specification of the risk that may occur to the computer, computer data, computer system, other information related to computer system, property, and life and body of a person;

(2) measures to prevent the risk that may occur;

(3) measures to examine and monitor the Cyber Threats;

(4) measures to respond when the Cyber Threats are detected;

(5) measures to remedy and restore the damage occurred from a Cyber Threat.

Section 14 In order to act in accordance with section 13 paragraph one (2) to cope with Cyber Threats in a timely manner, the CRC may assign the Minister of the Digital Economy and Society, Supreme Commander, and other directors as determined by the CRC to jointly perform such duty, and may determine that the Supervising or Regulating Organization and the threatened Organization of Critical Information Infrastructure shall join in order to act, coordinate, and provide support.

The performance under paragraph one shall be in accordance with the rules prescribed by the CRC.

Section 15 The provision of section 6, section 7, and section 8 shall be applied to the honorary directors in the CRC *mutatis mutandis*.

Section 16 The CRC shall have the power to appoint the sub-committee to perform any tasks as assigned by the CRC.

Section 17 The meeting of the CRC and the sub-committee shall be in accordance with the rules as determined by the CRC, where the meeting may proceed via electronic means or other means.

Section 18 The chairperson, the chairman of the sub-committee, and the sub-committee which the CRC appointed shall receive a meeting allowance or other compensation in accordance with the criteria determined by the Cabinet.

Section 19 In order to perform the duties in accordance with this Act, the Competent Official shall present his/her identification card to the relevant person.

In the appointment of the Competent Official, the Minister shall consider appointing a person with the knowledge and expertise in Maintaining Cybersecurity to be the Competent Official to perform any tasks under this Act. The level of such knowledge and expertise of the Competent Official shall be in accordance with the notification prescribed by the CRC.

The identification card issued to the Competent Official shall be in accordance with the notification prescribed by the CRC.

Chapter 2

Office of the National Cybersecurity Committee

Section 20 There shall be an Office of the National Cybersecurity Committee as a Government Agency who is a juristic person and not a government sector entity under the laws governing the administration or a state enterprise under the law on budget procedures or other laws.

Section 21 The operation of the Office is not regulated by the labor protection law, labor relation law, social security law, and compensation fund law. However, officers and employees of the Office shall receive compensation not less than that specified under the labor protection law, social security law, and compensation fund law.

Section 22 The Office shall be responsible for administrative, academic, meeting, and secretarial tasks of the Committee and the CRC, and shall also have the duties and powers to:

(1) suggest and support preparation of the policy and plan on Maintaining Cybersecurity and the operational plan for Maintaining Cybersecurity in accordance with section 9 to the Committee;

(2) prepare the Code of Practice and standard framework in Maintaining Cybersecurity in accordance with section 13 paragraph one (4), proposed to the CRC for the approval;

(3) coordinate the acts of Maintaining Cybersecurity of Organization of Critical Information Infrastructure in accordance with section 53 and section 54;

(4) coordinate and cooperate in the establishment of coordinating agencies for Maintaining Cybersecurity in the country and foreign countries with respect to Cybersecurity Incidents and determining Cybersecurity Solutions;

(5) act and coordinate with the Government Agency and private organizations in order to respond and cope with the Cyber Threats as assigned by the Committee;

(6) monitor the risk of occurrence of Cyber Threats, follow, analyze, and process information in relation to the Cyber Threats and the alerts on the Cyber Threats;

(7) perform, coordinate, support, and assist relevant agencies in complying with the policy and plan on Maintaining Cybersecurity, the operational plan for Maintaining Cybersecurity, and the measures to prevent, cope with, and mitigate the risks at Cyber Threats or as ordered by the Committee;

(8) act and cooperate or assist in preventing, coping with, and mitigating the risks of Cyber Threats, especially Cyber Threats that affect or occur in relation to the Critical Information Infrastructure;

(9) strengthen the knowledge and understanding in Maintaining Cybersecurity, including to create awareness of the incidents regarding the Cyber Threats in order to have a practical operation in a manner that is integrated and up-to-date;

(10) act as central point of collection and analysis of data regarding Maintaining Cybersecurity of the country, and disseminating the information related to cybersecurity risks and incidents to Government Agencies and private organizations;

(11) act as the central coordinator between the institution regarding Maintaining Cybersecurity of Government Agencies and private organizations, both in the country and in foreign countries;

(12) make agreements and cooperate with organizations or institutions both in the country and in foreign countries for the operation in accordance with the duty and power of the Office, upon receiving approval from the Committee;

(13) study and research necessary information required for Maintaining Cybersecurity, in order to prepare recommendations on measures for Maintaining Cybersecurity, including providing relevant agencies with training and practice for coping with the Cyber Threats;

(14) enhance, support, and act in order to disseminate knowledge regarding Maintaining Cybersecurity, and provide trainings to enhance the skills and expertise in performing duties in relation to Maintaining Cybersecurity;

(15) report the progress and situation for the execution of this Act including the problems, obstacles, and proposal to the Committee to consider to proceed according to the period as determined by the Committee;

(16) perform any other task related to Maintaining Cybersecurity of the country as assigned by the Committee or the Cabinet.

For the benefit of acting according to the duties and powers in accordance with (6), the Office shall establish a national coordinating agency for maintaining the security of computer systems as an internal department of the Office, which shall have duties and powers as determined by the Committee.

Section 23 In the operation of the Office, aside from the duties and powers under section 22, the Office shall have the following general duties and powers to:

(1) have the ownership, possession, and property rights;

(2) establish any rights or enter into any juristic acts that shall bind the properties as well as enter into any other juristic acts for the benefit of the operation of the Office;

(3) prepare and provide funding in support of the operation of the Office;

(4) collect fees, maintenance fees, compensation, or service fees for its operation, in accordance with the criteria and rate as determined by the Office under the approval of the CMO;

(5) perform any other tasks determined under law to be the duties and powers of the Office, or as assigned by the Committee or the CMO.

Section 24 The capital and properties for the operation of the Office shall consist of:

(1) the initial funding assigned by the government under section 81 paragraph one and the money and properties transferred under section 82;

(2) general subsidiaries appropriately allocated by the government on an annual basis;

(3) general subsidiaries from Government Agencies both inside and outside the country, or international government organizations;

(4) fees, maintenance fees, compensation, service fees, or income from performing duties and powers of the Office;

(5) fruit from money or income from the properties of the Office.

Money and properties of the Office under paragraph one must be provided to the treasury as national revenue.

Section 25 There shall be a Committee Managing the Office of the National Cybersecurity Committee, abbreviated as "CMO," to supervise the general administration of the Office, consisting of the Minister of the Digital Economy and Society as the chairperson, Permanent Secretary of the Ministry of Digital Economy and Society, Director General of the Controller General's Department, the Secretary-General of the Civil Service Commission, the Secretary-General of the Office of the Public Sector Development, and honorary directors not exceeding six persons to be directors.

The Secretary-General shall be a director and secretary, and the Secretary-General shall appoint assistant secretaries from the officials of the Office not exceeding two persons.

The honorary directors under paragraph one shall be appointed by the Cabinet among the persons who have knowledge, expertise, and remarkable competency in Maintaining Cybersecurity, information technology and communications, economics, social science, law, business management, or other relevant aspects which are beneficial to the operation of the CMO in accordance with the criteria and method as determined by the Committee.

Section 6 and section 8 shall be applied *mutatis mutandis* to the honorary committees.

Section 26 The honorary directors of the CMO shall have a four-year term for each office.

In case of the additional appointment of the honorary directors or the replacement of the honorary directors who has vacated the office prior to the expired term, the Minister may appoint the additional honorary directors or in replacement of the vacant office. An honorary director who has been additionally appointed or appointed in replacement of the vacant office shall stay in the office for the remaining period of the term of the appointed honorary director.

When a term expires in accordance with paragraph one, if the new honorary director has yet to be appointed, the honorary director whose term has expired shall remain in the office to further perform the duties until a new honorary director is appointed.

Section 27 The CMO shall have the following duties and powers to:

(1) determine the management policy and approve the operational plan of the Office;

(2) issue regulations regarding the organization, finance, human resources, general management, stock, internal inspection, and other support and welfare of the Office;

(3) approve the payment plan and annual expense budget of the Office;

(4) control the management and operation of the Office and Secretary-General in accordance with this Act and other relevant laws;

(5) analyze the administrative order of the Secretary-General in relation to the management of the Office;

(6) evaluate the result of the operation of the Office and the execution of the Secretary-General;

(7) perform any other task as specified under this Act or other relevant laws as duties and powers of the CMO or as assigned by the Committee or the Cabinet.

In performing the duties under paragraph one, the CMO may appoint a sub-committee to consider, suggest, or perform any act as assigned by the CMO, with performance of such duties and meetings to be in accordance with the criteria and method determined by the CMO.

The CMO may appoint the honorary committee who has expertise in aspects beneficial to the operation of the Office as a consultant of the CMO under the criteria and method determined by the Committee.

Section 28 The chairperson and the director, the chairman of the sub-committee, and the sub-committee appointed by the CMO shall receive a meeting allowance and other compensation in accordance with the rules determined by the Committee.

Section 29 The Office shall have a Secretary-General responsible for the operation of the Office and being a supervisor of the officers and employees of the Office.

Section 30 A Secretary-General shall have the following qualifications:

(1) have Thai nationality;
(2) not be under 35 years of age but not over 60 years of age;
(3) have knowledge, competencies, and experience in fields related to the mission of the Office and management skills.

Section 31 A person having any of the following characteristics shall be prohibited from being a Secretary-General:
(1) be a bankrupted person or used to be a dishonestly bankrupted person;
(2) be an incompetent or quasi-incompetent person;
(3) having been previously imprisoned by the final court judgement regardless the actual imprisonment unless the offences committed by negligence or misdemeanors;
(4) be a civil servant, officer, or employee of a government authority, state enterprise, or other Government Agency or local department;
(5) be or having been previously a political official, person holding political position, local councilor, or local administer unless having vacated from the office for not less than one year;
(6) be or having been previously a director or a person in other positions in the political party, or an officer of the political party unless having vacated from the office for not less than one year;
(7) having been previously dismissed, fired, or removed from an official position in a previous organization on grounds of dishonest performance of duties or severe wrongful conduct, or removed from office;
(8) having been previously removed on grounds of not passing a performance evaluation under section 35 (5).

Section 32 The Committee shall determine the salary and other compensation of a Secretary-General in accordance with the method determined by the Cabinet.

Section 33 A Secretary-General shall have a four-year term for each office.
A Secretary-General who has vacated the office due to expiration of the term may be reappointed, but not exceeding two terms.

Section 34 Each year, there shall be a performance evaluation of a Secretary-General in accordance with the period and method determined by the Committee.

Section 35 Apart from the expiration of term, a Secretary-General vacates office upon:
(1) death;
(2) resignation;
(3) lacking qualifications as specified in section 30 or possessing prohibited characteristics as specified in section 31;
(4) resolution for removal passed by the Committee on grounds of unsatisfactory or dishonest performance of duties, disgraceful behavior, or incapacity;
(5) removal from the Committee based on failure to pass the performance evaluation;
(6) vacating in accordance with the terms specified under the employment agreement or agreement between the Committee and the Secretary-General.

Section 36 A Secretary-General under the supervision of the Committee, CRC, and

CMO shall comply with the orders of the Committee, CRC, and CMO under the duties and powers as follows:

(1) manage the operation of the Office to accomplish in accordance with the mission of the Office, and with the policy and plan on Maintaining Cybersecurity, the operational plan for Maintaining Cybersecurity, the policies of the Cabinet and the Committee, and regulations, policies, resolutions and notifications of the CMO;

(2) issue regulations under the policy of the Committee and CRC that are not contrary to the law, Cabinet resolutions, and the regulations, policies, resolutions, and notifications determined by the Committee and CRC;

(3) be a supervisor of the officers and employees of the Office and evaluate the performances of officers and employees of the Office in accordance with the regulations of the CMO and the rules of the Office;

(4) appoint the deputy Secretary-General or assistant of the Secretary-General as approved by the Committee to be an assistant in the operation of the Secretary-General as assigned by the Secretary-General;

(5) assign, appoint, promote, demote, deduct the salaries or wages of, execute disciplinary action against officers and employees of the Office, and remove officers and employees of the Office in accordance with the regulations determined by the CMO and the rules of the Office;

(6) perform any other task as specified under the regulations, policies, resolutions, or notifications of the CMO or the CRC.

For the operation of the Office in relation to external personnel, the Secretary-General shall be the representative of the Office, under the scope set forth by the Committee.

The Secretary-General may assign its power to any person under the Office to perform a specific task under the regulations determined by the CMO.

In case that there is no Secretary-General or the Secretary-General cannot perform his or her duties, the deputy Secretary-General in order of the seniority shall be in charge. If there is no deputy Secretary-General or the deputy Secretary-General cannot execute the duties, the Committee shall appoint an appropriate person to do so.

Section 37 The accounts of the Office shall be prepared in accordance with the forms and criteria determined by the CMO, taking into account international principles and accounting standards.

Section 38 The Office shall prepare and submit a financial statement and accounting report to an auditor within ninety days from end of the fiscal year.

The Office of the Auditor General or the auditor authorized by the Office of the Auditor General shall approve the auditor of the Office and appraise the results of expenses and assets of the Office in each fiscal year, and shall prepare the result of the audit to be submitted to the CMO for approval.

Section 39 The Office shall prepare an annual report to be submitted to the Committee within one hundred and eighty days from the end of the fiscal year, and shall disclose the annual report to the public.

The annual report under paragraph one shall describe the details of balance sheets as approved by an auditor, the performance of the Office, and the outcome of the performance evaluation of the Office during the previous fiscal year.

The evaluation of the Office under paragraph two shall be done by an external person who has been approved by the CMO.

Section 40 The Cabinet shall have the power to generally supervise the operation of the Office in accordance with the duties and powers of the Office, the laws, national strategies, policies and plans of the government, and relevant Cabinet resolutions. In the light of this, the Cabinet shall have the power to order the Secretary-General to clarify facts, comment, or prepare the report, and cease operations of the Office that are against the duties and powers of the Office, the laws, national strategies, policies and plans of the government, or the relevant Cabinet resolutions, including to order an investigation of the facts regarding operations of the Office.

Chapter 3
Maintaining Cybersecurity

Part 1
Policies and plans

Section 41 Maintaining Cybersecurity shall take into consideration the unity and integration of the operation of Government Agencies and private organizations, and shall align with the national policy and plan regarding the digital development for economy and society in accordance with the laws regarding the digital development for economy and society, and the policy and master plan which are related to maintaining the security of the National Security Council.

The operation on Maintaining Cybersecurity shall aim to create the capability to prevent, cope with, and mitigate risks from Cyber Threats, especially in protecting the Critical Information Infrastructure of the country.

Section 42 The policy and plan on Maintaining Cybersecurity shall at least contain the following objectives and approaches:

(1) integration of management in Maintaining Cybersecurity of the country;
(2) establishment of measures and mechanisms to develop capability to prevent, cope with, and mitigate the risks from Cyber Threats;
(3) establishment of measures to protect the Critical Information Infrastructure of the country;
(4) cooperation between the public and private sector, and international cooperation for Maintaining Cybersecurity;
(5) research and development of technology and knowledge related to Maintaining Cybersecurity;
(6) development of personnel and experts in Maintaining Cybersecurity, both in the public and the private sector;
(7) creation of awareness and knowledge in Maintaining Cybersecurity;
(8) development of rules and laws for Maintaining Cybersecurity.

Section 43 The Committee shall prepare a policy and plan for Maintaining Cybersecurity in accordance with section 42 to propose to the Cabinet for approval, which shall be published in the *Government Gazette*. Once published, Government Agencies, Supervising or Regulating Organizations, and Organizations of Critical Information Infrastructure as determined in the plan on Maintaining Cybersecurity shall take action to be in accordance with such policy and plan.

In preparing the policy and plan under paragraph one, the Office shall hold a hearing or meeting with the Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure.

Section 44 The Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure shall prepare a Code of Practice and standard framework for Maintaining Cybersecurity of each organization in accordance with the policy and plan on Maintaining Cybersecurity without delay.

The Code of Practice for Maintaining Cybersecurity under paragraph one, at least, shall consist of the following:

(1) the plan for examining and assessing risks related to Maintaining Cybersecurity by an examiner, internal auditor, or independent external auditor, at least once per year;

(2) the plan for coping with Cyber Threats.

For the benefit of preparing the Code of Practice for Maintaining Cybersecurity in paragraph one, the Office, upon the approval of the Committee, shall prepare a Code of Practice and standard framework for the Government Agency, Supervising or Regulating Organization, or Organization of Critical Information Infrastructure to use as a guideline to prepare or exercise as a Code of Practice of the Government Agency, Supervising or Regulating Organization, or Organization of Critical Information Infrastructure. In case such organizations do not yet have or have but incomplete or is not in accordance with the Code of Practice and standard framework, such Code of Practice and standard framework shall be enforced.

Part 2
Management

Section 45 The Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure have a duty to prevent, cope with, and mitigate risks from Cyber Threats in accordance with the Code of Practice and standard framework for Maintaining Cybersecurity of each organization and shall act in order to be in compliance with the Code of Practice and standard framework for Maintaining Cybersecurity in accordance with section 13 paragraph one (4).

In case the Government Agency, Supervising or Regulating Organization, or Organization of Critical Information Infrastructure could not act or comply in accordance with paragraph one, the Office may grant assistance in the personnel or technological aspects to such organization as requested.

Section 46 For the benefit of Maintaining Cybersecurity, the Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure shall notify the name of executive officials and operational officials for the coordination of Maintaining Cybersecurity to the Office.

In the event there is a change to the officials under paragraph one, the Government Agency, Supervising or Regulating Organization, and Organization of Critical Information Infrastructure shall notify the Office without delay.

Section 47 In case the performance of the duties in accordance with this Act requires knowledge and expertise, the Committee or the CRC may assign the Secretary-General to hire an expert as appropriate for each specific task.

The expert in paragraph one shall have appropriate qualifications or experience in accordance with the notification prescribed by the Committee.

The Secretary-General shall issue an expert identification card to the appointed person. When performing duties, such person shall display the identification card as an expert and, once duties are completed, shall return the identification card to the Office without delay.

Part 3
Critical Information Infrastructure

Section 48 The Critical Information Infrastructure is an operation which are important to national security, military security, economic security, and public order in the country, and it shall be the duty of the Office to assist and provide assistance to prevent, cope with, and mitigate risks from Cyber Threats, especially, Cyber Threats that affect or occur in relation to the Critical Information Infrastructure.

Section 49 The Committee shall have the power to prescribe in a notification the characteristics of the organizations that have a mission or provide services in the following aspects, as an Organization of Critical Information Infrastructure:

(1) national security;
(2) substantive public service;
(3) banking and finance;
(4) information technology and telecommunications;
(5) transportation and logistics;
(6) energy and public utilities;
(7) public health;
(8) others as prescribed by the Committee.

The consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be published in the *Government Gazette*. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate.

Section 50 The Committee has the power to prescribe the characteristics, duties, and responsibilities of the coordinating agency for maintaining the security of computer systems for the Organization of Critical Information Infrastructure of section 49 to coordinate, monitor, cope with, and resolve Cyber Threats by prescribing the Government Agency that is ready or such Critical Information Infrastructure Supervising or Regulating Organization to perform such duties for the Organization of Critical Information Infrastructure in accordance with section 49, in whole or in part.

Consideration for the prescription of such mission or services under paragraph one shall be in accordance with the rules prescribed by the Committee, which shall be published in the *Government Gazette*. The Committee shall consider and review such prescription of the mission or services on a case-by-case basis as appropriate.

Section 51 In the event of any inquiries or claims related to the characteristics of the organizations having the mission or providing the services as prescribed in accordance with section 49 or section 50, the Committee shall make the final decision.

Section 52 For the benefit of coordination, the Organization of Critical Information

Infrastructure shall notify the name and contact information of the owner, the person possessing the computer, and the person monitoring the computer system to the Office, its Supervising or Regulating Organization, and the organization under section 50, within thirty days from the date the Committee prescribes the notification in accordance with section 49 paragraph two and section 50 paragraph two, or from the date the Committee issues a final judgement in accordance with section 51, as the case may be; the owner, the person possessing the computer, and the person monitoring the computer system shall at least be a person responsible for the management of such Organization of Critical Information Infrastructure.

In case there is any change to the owner, the person possessing the computer and the person monitoring the computer system in accordance with paragraph one, notice of change to the relevant organizations under paragraph one shall be given not less than seven days in advance, unless there is reasonable cause which is inevitable, it shall be notified without delay.

Section 53 In the operation of Maintaining Cybersecurity of the Organization of Critical Information Infrastructure, the Supervising or Regulating Organization shall examine the minimum cybersecurity standard of the Organization of Critical Information Infrastructure under its supervision. If found that Organization of Critical Information Infrastructure does not comply with the standards, the Supervising or Regulating Organization shall notify the Organization of Critical Information Infrastructure which is below the standards to make correction in order to meet the standards without delay. If such Organization of Critical Information Infrastructure neglects or fails to comply within the period prescribed by the Supervising or Regulating Organization, the Supervising or Regulating Organization shall notify the CRC for consideration without delay.

Upon receipt of notification under paragraph one, if the CRC considers and views that there is such reason and which may cause a Cyber Threat, the CRC may perform the following:

(1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or the Organization of Critical Information Infrastructure to correct and comply with the standards without delay;

(2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person monitoring the computer system of the Organization of Critical Information Infrastructure to make correction and comply with the standards without delay.

The Secretary-General shall monitor to ensure compliance of paragraph two.

Section 54 The Organization of Critical Information Infrastructure shall conduct risk assessment on Maintaining Cybersecurity by having an examiner, including examination in the cybersecurity aspect by the information security auditor, internal auditor or external independent auditor, at least once per year.

The Organization of Critical Information Infrastructure shall submit a summary report of the operation result to the Office within thirty days after the operation has been finished.

Section 55 In case the CRC views that the risk assessment on Maintaining Cybersecurity or the examination in the cybersecurity aspect in accordance with section 54 is not in compliance with the standards according to the report of the Supervising or Regulating Organization, the CRC shall order the Organization of Critical Information Infrastructure to conduct the risk assessment again to be in accordance with the standards, or proceed with the examination in other aspects that may affect the Critical Information Infrastructure.

In case the Organization of Critical Information Infrastructure has already conducted the

risk assessment on Maintaining Cybersecurity or examination in the cybersecurity aspect of paragraph one but the CRC views that it is not in compliance with the standards, CRC may perform the following:

(1) in case of a Government Agency, the CRC shall notify the chief executive of the agency to exercise executive power to issue an order to the Government Agency or Organization of Critical Information Infrastructure to correct and comply with the standards without delay;

(2) in case of a private organization, the CRC shall notify the chief executive of the organization, the person possessing the computer, and the person monitoring the computer system of the Organization of Critical Information Infrastructure to make correction and comply with the standards without delay.

The Secretary-General shall monitor to ensure compliance of paragraph two.

Section 56 The Organization of Critical Information Infrastructure shall establish a mechanism or process to monitor Cyber Threats or Cybersecurity Incidents which relates to its Critical Information Infrastructure in accordance with the standards as determined by the Supervising or Regulating Organization and in accordance with Code of Practice, including the system of Cybersecurity Solution as determined by the Committee or the CRC, and shall participate in the assessment on the readiness in coping with Cyber Threats as held by the Office.

Section 57 In the event of a Cyber Threat significantly occurring to the system of the Organization of Critical Information Infrastructure, the Organization of Critical Information Infrastructure shall report to the Office and the Supervising or Regulating Organization and cope with the Cyber Threats as prescribed in Part 4, the CRC may prescribe criteria and method of the reporting.

Part 4
Coping with Cyber Threats

Section 58 In the case there is or may be a Cyber Threat to an information system that is under the responsibility of a Government Agency or an Organization of Critical Information Infrastructure, such organization shall examine its related information, computer data, and the computer system, including the surrounding circumstances to assess whether a Cyber Threat has occurred. If the examination results show that there is or may be a Cyber Threat, the organization shall prevent, cope with, and mitigate the risks from such Cyber Threat in accordance with the Code of Practice and standard framework in Maintaining Cybersecurity and shall notify the Office and its Supervising or Regulating Organization without delay.

In case the agency or organization, or any person, finds an obstacle or issues in preventing, coping with, or mitigating the risks from a Cyber Threat, such agency, or organization or person may request assistance from the Office.

Section 59 When it appears to the Supervising or the Regulating Organization, or when the Supervising or the Regulating organization is notified of an incident in accordance with section 58, the Supervising or Regulating Organization in cooperation with the organization under section 50 shall gather information, examine, analyze the situation, and evaluate the effects related to the Cyber Threat and shall perform the following:

(1) support and grant assistance to the Government Agency or Organization of Critical

Information Infrastructure under the supervisor or regulation and cooperate and coordinate with the Office to prevent, cope with, and mitigate the risks from the Cyber Threat;

(2) notify the Government Agency or Organization of Critical Information Infrastructure under its supervision or regulation, including other relevant Government Agencies or Organizations of Critical Information Infrastructure without delay.

Section 60 In considering to exercise power to prevent Cyber Threats, the Committee will determine the type of Cyber Threat as classed into three levels, as follows:

(1) a Cyber Threat at a non-critical level means a Cyber Threat with significant risk at a level which causes the computer system of the country's Organization of Critical Information Infrastructure to be compromised;

(2) a Cyber Threat at a critical level means a Cyber Threat with the nature of having significant increase in computer system, computer, or computer data attacks, with the aim to attack the Organization of Critical Information Infrastructure of the country, and such attack has the effect of causing damage to the computer system of the information technology infrastructure related to the operation of the Organization of Critical Information Infrastructure of the country, public stability, international relations, national defense, economy, public health, public safety, or the public order of the people, such that it could not operate or provide service;

(3) a Cyber Threat at a crisis level means a Cyber Threat in a crisis level of the following nature;

(a) is a Cyber Threat occurring from a computer system, computer, computer data attacks in a level higher than the Cyber Threats in a critical level, which cause severe effect to Critical Information Infrastructure of the country in a large-scale and which causes the whole operation of Government Agency or the provision of service of Organization of Critical Information Infrastructure to fail, such that the state could not control the operation center of the state's computer system, or the normal remedial measures for Cyber Threat could not resolve the issue and there is risk of spreading to other critical infrastructure of the country, which may cause death to many people or cause a great amount of computer system, computer, and computer data to be destroyed in a large-scale on a national level;

(b) is a Cyber Threat that affects or may affect the public order or is a threat to public security or may cause the country or part of the country to be in a critical situation, or an offense regarding terrorism under the Penal Code, battling or war, which an urgent measure is required to maintain the democratic form of government with the King as the Head of the State in accordance with the Constitution of the Kingdom of Thailand, sovereignty and the integrity of the territory, national benefit, compliance with the laws, public safety, normal living of the public, protection of freedom and rights, public order or benefit, or the protection or remedy of damages from the public disaster that is emergency and critical.

The details of the characteristics of the Cyber Threats, the measures to prevent, cope with, assess, suppress, and suspend of the Cyber Threats in each level shall be in accordance with the notification prescribed by the Committee.

Section 61 When it appears to the CRC that there is or there may be a Cyber Threat

at a critical level, the CRC shall issue an order to the Office to perform the following:

(1) gather information, or relevant documentary evidence, witness, material evidence to analyze the situation, and evaluate the effects from Cyber Threats;

(2) support, assist, and participate in the prevention, coping with, and mitigation of risks from Cyber Threats;

(3) prevent Cybersecurity Incidents which occurred from Cyber Threats, suggest or issue an order to use the solution system to maintain cybersecurity, including finding the approach for countermeasure or solution regarding cybersecurity;

(4) support such that the Office and the relevant organizations, both the public and private sector, to provide assistance and participate in the prevention, coping with, and mitigation of risks from the Cyber Threats occurred;

(5) notify of the Cyber Threat to be informed in general, as necessary and appropriate, taking into consideration the situation, severity, and effect from such Cyber Threat;

(6) facilitate in coordinating between relevant Government Agency and private organization to deal with risks and incidents related to cybersecurity.

Section 62 In operations in accordance with section 61, for the benefit of analyzing the situation and evaluating the effects from Cyber Threats, the Secretary-General shall order the Competent Officials to:

(1) issue a letter requesting cooperation from the relevant persons to provide information within an appropriate period and at the prescribed place, or provide information in writing related to the Cyber Threat;

(2) issue a letter requesting for information, documents, or copy of the information or documents in the possession of other person which is beneficial to the operation;

(3) inquire the persons who has knowledge and understanding of the facts and situations which are related to the Cyber Threat;

(4) enter into a property or place of business which is or may be related to the Cyber Threat of a related person or organization, with consent from the person in possession of such place.

Any person providing information in accordance with paragraph one, which acts in good faith, shall receive protection and shall not be deemed a wrongful act or a breach of a contract.

Section 63 In case of necessity to prevent, cope with, and mitigate risks from a Cyber Threat, the CRC shall order the Government Agency to provide information, support its personnel, or use electronic devices under its possession in relation to Maintaining Cybersecurity.

The CRC shall ensure that there shall be no use of information under paragraph one that may cause damages and the CRC is responsible for the compensation for the personal, expenses, damages occurred from the use of such electronic devices.

Paragraph one and two shall also be applied to the requests to private organization, upon the consent of such private organization.

Section 64 In case there is or may be a Cyber Threat at a critical level, the CRC shall prevent, cope with, and mitigate risks from the Cyber Threat and conduct necessary measures.

In the operation under paragraph one, the CRC shall issue a letter to the Government Agency which relates to Maintaining Cybersecurity to act or omit any act to prevent, cope with, or mitigate risks from the Cyber Threat properly and efficiently, in accordance with the guideline prescribed by the CRC, including integrating the operation to control, terminate, or mitigate the

effect caused by the Cyber Threat in a timely manner.

The Secretary-General shall report the operation in accordance with this Section to the CRC constantly and when such Cyber Threat ends, the Secretary-General shall report the operation result to the CRC without delay.

Section 65 In coping with and to remedy the damages from a Cyber Threat at a critical level, the CRC has the power to order, only as necessary to prevent the Cyber Threat, the owner, the person possessing the computer, or the user of a computer or a computer system or a person monitoring the computer system, which has a reasonable cause to believe that he/she is related to the Cyber Threat or is affected by the Cyber Threat to conduct the following acts:

(1) monitor the computer or computer system during a certain period of time;

(2) examine the computer or computer system to find an error that affects Maintaining Cybersecurity, analyze the situation, and evaluate the effects from the Cyber Threat;

(3) conduct a measure rectifying the Cyber Threat to handle vulnerabilities or remove unwanted programs or terminate and remedy the Cyber Threat that are operating;

(4) maintain the status of the computer data or computer system via any methods to operate the computer forensic science;

(5) access relevant computer data or computer system or other information related to the computer system only to the extent it is necessary to prevent Cyber Threat.

In case of necessity to access information under (5), the CRC shall assign the Secretary-General to submit the motion to the Competent Court to order the owner, the person possessing the computer, the user of the computer or computer system or a person monitoring the computer system in accordance with paragraph one to comply with the motion. The motion submitted to the Court shall specify the cause to believe that a person is performing or will perform an act that cause Cyber Threat in a critical level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.

Section 66 In preventing, coping with, or mitigating the risks from Cyber Threats in a critical level, the CRC has the power to order a Competent Official, only to the extent that it is necessary to prevent the Cyber Threat, to do the following:

(1) enter into a place to examine, with a letter informing the appropriate reason to the owner or the occupier to examine such place. If there is a cause to believe that there is a computer or computer system related to the Cyber Threat or is affected from the Cyber Threat;

(2) access the computer data, computer system, or other data related to the computer system, copy, or filter/screen information data or computer program which has a reason to believe that is related to or affected by the Cyber Threat;

(3) test the operation of the computer or computer system which has a reason to believe that is related to or affected by the Cyber Threat or has been used to search any information from the inside or taking advantage of the computer or computer system;

(4) seize or freeze a computer, a computer system, or any equipment, only to the extent it is necessary, which has a reason to suspect that is related to the Cyber Threat for the examination or analysis, for not more than thirty days. Once such period is over, computer or any equipment shall be returned to the owner or the person possessing the computer immediately after the examination or analysis is finished.

In operating in accordance with (2), (3), and (4), the CRC may submit a motion to the Competent Court to order the officers to comply with the motion. The motion submitted to the

Court shall specify the cause to believe that a person is performing or will perform an act that will cause a Cyber Threat at a critical level. The motion shall be submitted as emergency hearing motion and shall be considered by the Court without delay.

Section 67 In case there is a Cyber Threat at a crisis level, it shall be in the duty and power of the National Security Council in Maintaining Cybersecurity under the laws on National Security Council and other relevant laws.

Section 68 In case it is urgent and necessary and the Cyber Threat is at a crisis level, the Committee may assign to the Secretary-General the power to act, only to the extent it is necessary to prevent and remedy the damages in advance, and the motion to the Court is not required to be submitted. However, after such operations, the details of the operations shall be notified to the Competent Court without delay.

In a critical or crisis case, for the benefit of preventing, assessing, coping with, suppressing, suspending, and mitigating the risks from the Cyber Threat, the Secretary-General, upon the approval of the Committee or CRC, shall have the power to request real-time information from a person related to the Cyber Threat. Such person shall cooperate with and facilitate the Committee or the CRC without delay.

Section 69 A person receiving an order related to coping with a Cyber Threat may only appeal such order for Cyber Threats at a non-critical level.

Chapter 4
Penalty Provisions

Section 70 The officers under this Act shall not disclose or send computer data, computer traffic data, other data related to the computer system, or data of the users obtained from this Act to any person. Any officer violating shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both.

Paragraph one shall not apply to act for the benefit of litigation against an offender under this Act or an offender under other laws or for the benefit of the litigation against the officer related to the exercising of unlawful authority.

Section 71 Any officer under this Act negligently causing other persons to know computer data, computer traffic data, data of the users, or other data related to the computer system obtained from this Act, shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.

Section 72 Any person who knows computer data, computer traffic data, data of the users, or data related to the computer system that the officer has obtained from this Act and unlawfully discloses such data to any person shall be subject to imprisonment not exceeding two years, a fine not exceeding Baht forty thousand, or both.

Section 73 Any Organization of Critical Information Infrastructure not reporting a Cyber Threat incident in accordance with section 57 without reasonable cause shall be subject to a fine not exceeding Baht two hundred thousand.

Section 74 Any person not complying with the summoning letter of the Competent Officials, or not sending information to the Competent Official in accordance with section 62 (1)

or (2) without a reasonable cause, as the case may be, shall be subject to a fine not exceeding Baht one hundred thousand.

Section 75 Any person violating or not complying with an order of the CRC in accordance with section 65 (1) (2) without a reasonable cause shall be subject to a fine not exceeding Baht three hundred thousand and a daily fine not exceeding Baht ten thousand from the date on which the CRC issues the orders until compliance.

Any person violating or not complying with the order of the CRC in accordance with section 65 (3) and (4) or not complying with the court order in accordance with section 65 (5) shall be subject to imprisonment not exceeding one year, a fine not exceeding Baht twenty thousand, or both.

Section 76 Any person disrupting or not complying with an orders of the CRC or the Competent Official performing its duty in accordance with the CRC's order in accordance with section 66 (1), or not complying with the Court order in accordance with section 66 (2), (3), or (4), without a reasonable cause shall be subject to imprisonment not exceeding three years, a fine not exceeding Baht sixty thousand, or both.

Section 77 In case the person committing an offense under this Act is a juristic person, if such offense is a result of the order or the act of a director or a manager or any person responsible for the operation of such juristic person or in case such person has the duty to order or act and omit to order or act, causing the juristic person to commit an offense, such person shall be liable for the penalties prescribed for such offense.

Transitory Provisions

Section 78 At the beginning, the Committee shall consist of the chairperson and the committees under section 5 (1) and (2) and the Secretary-General of the National Cybersecurity Committee shall be a committee and secretary in order to temporarily conduct the duty only to the extent necessary and shall appoint the honorary committees of the Committee under section 5 (3) within ninety days from the date this Act enters into force.

In appointing the honorary director under paragraph one, the Minister of Digital Economy and Society may nominate list of individuals to the Cabinet for considering on appointing as honorary director.

Section 79 The CRC and the CMO shall be established within ninety days from the date of appointment of the honorary director of the Committee under section 78.

The Secretary-General under this Act shall be appointed within ninety days from the date the establishment of the Office has been complete under section 80.

Section 80 Establishment of the Office shall be completed in order to perform its duty in accordance with this Act within one year from the date this Act enters into force.

While the establishment of the Office has not been completed, the Office of the Permanent Secretary, Ministry of Digital Economy and Society, shall perform the duty of the Office under this Act, and the Permanent Secretary of the Ministry of Digital Economy and Society shall perform the duty as the Secretary-General until there is an appointment of the Secretary-General in accordance with section 79 paragraph two.

Section 81 At the beginning, the Cabinet shall assign an initial funding to the Office

as necessary.

The Minister shall propose to the Cabinet for consideration the public servant, official, personnel, officer, or the person performing any other task in a Government Agency to work in the Office temporarily within the period prescribed by the Cabinet.

The public servant, official, personnel, officer, or the person performing any other task in a Government Agency operating in the Office temporarily in accordance to paragraph two shall not be rid of their current status and shall receive salary or wage, as the case may be, from the same organization. the CRC may prescribe special compensation for the public servant, officials, personnel, officer, or the person performing any other task in a Government Agency in accordance with paragraph two during the operation in the Office.

Within one hundred and eighty days from the date the establishment of the Office has been completed, the Office shall select the public servant, official, personnel, officer, or the person performing any other task in a Government Agency to be placed as its personnel.

The public servant, official, personnel, officer, or the person performing any other task in a Government Agency who has been selected and placed in accordance with paragraph four shall be entitled to count the duration of employment at the previous agency in continuation to the duration of employment in the Office under this Act.

Section 82 When this Act enters into effect, the Minister shall present the operating Cabinet to approve the transfer of all the duties, power, business, properties, rights, debts, and budgets of all the tasks related to Maintaining Cybersecurity of the Permanent Secretary, Ministry of Digital Economy and Society and the Electronic Transactions Development Agency, which exist prior to the day this Act enters into force, to the Office, in accordance with this Act.

Section 83 Issuance of the regulations, rules, and notifications in accordance with this Act shall be completed within one year from the date this Act enters into force. If such cannot be carried out, the Minister shall report the reasons that is could not be carried out to the Cabinet

Countersigned by

General Prayut Chan-o-cha

Prime Minister

Remarks :- The reason for the enactment of this Act is that nowadays the provision of services or application of the computer networks, the internet, telecommunication networks, or general satellite services are currently under the risk of Cyber Threats which may threaten national security and public order in the country. In order to be able to simultaneously prevent or cope with Cyber Threats, it is deemed appropriate to determine the characteristics of the mission or services that are fundamental as critical information infrastructure, for both the government agency and private organization, which are necessary to be prevented, coped with, and mitigated from the risk of Cyber Threats, such that there is no adverse effects on security in varying aspects, including to have the competent authorities responsible for proceeding with the relevant tasks, coordinating between the government and private sectors regardless of the general situation or the situation which severely threatens security, and establishing operational plan and standards in maintaining cybersecurity in united and continuous manner. This will make the prevention and coping with cyber threats efficient and thus the Act is necessary to be enacted.