Content

Title：	Cyber Security Management Act Ch
Date：	2018.06.06
Legislative：	1.Enacted and promulgated a total twenty-three articles of the Act by Presidential Order Hua Zong 1 Yi Zi No. 10700060021 on June 6, 2018; The implementation date of the Act shall be stipulated by the competent authority. Issued by Executive Yuan Order yuan tai hu zi No. 1070217128 on December 5, 2018. The implementation date of the Act was stipulated on January 1, 2019.
Content：	Chapter I. General Provision Article 1 This Cyber Security Management Act (hereinafter referred to as the Act) is duly stipulated in an effort to positively carry out the national cyber security policy, accelerate the construction of environment for national cyber security to safeguard national security, and protect public interests of the entire society. Article 2 The competent authority over the Act is the Executive Yuan. Article 3 The terms under the Act are defined as follows: 1. Information and communication system: That refers to the system to be used to collect, control, transmit, store, circulate, delete information or to make other processing, using and sharing of such information. 2. Information and communication service: That refers to the service to be used to collect, control, transmit, store, circulate, delete information or to make other processing, using and sharing of such information. 3. Cyber security: That refers to such effort to prevent information and communication system or information from being unauthorized access, use, control, disclosure, damage, alteration, destruction or other infringement to assure the confidentiality, integrity and availability of information and system. 4. Cyber security incident: That refers to an event where the state of a system, service, or network is identified as having a potential violation of the cyber security policy or a failure of protective measures, which affects the functionality of the information and communication system and constitutes a threat against the cyber security policy. 5. Government agency: That refers to central, local government agency (institution) or public juristic person that exercises public power according to law, excluding military and intelligence agency. 6. Specific non-government agency: That refers to critical infrastructure provider, government-owned enterprises and government-endowed foundation. 7. Critical infrastructure: That refers to physical or virtual assets, systems or networks, the functions of which, once ceased to operate or their performance is reduced, may have a significant impact on national security, social and public interests, people's lives, or economic activities, and which are subject to regular inspection and announcement by the competent authorities. 8. Critical infrastructure provider: That refers to the ones who maintain or provide critical infrastructure either in whole or in part, as designated by the central authority in charge of relevant industry, which shall be submitted to the competent authority for ratification. 9. Government-endowed foundation: That refers to a foundation of which the operation and capital utilization plan of its funds shall be submitted to the Legislative Yuan in accordance with Paragraph 3 of Article 41 of the Budget Act and its annual budget statement shall be submitted to the

Legislative Yuan for deliberation in accordance with Paragraph 4 of the same Article.

Article 4
In an effort to promote cyber security, the government shall provide resources and integrate the strengths of the private sector and the industry to boost cyber security awareness of all people, and implement the following issues:
1. Cultivation of cyber security professionals.
2. Cyber security technology research and development, integration, application, and industry-academia cooperation, as well as interchange and cooperation with international community.
3. Development of cyber security industry.
4. Development of cyber security related software and hardware specifications, relevant services and verification mechanism.
Issues Promotion in the preceding Paragraph shall be stipulated by the competent authority under the national cyber security development program.

Article 5
The competent authority shall plan and promote the national cyber security policy, and the cyber security technology development, international interchange and cooperation, and the comprehensive cyber security protection relevant undertakings, as well as regularly announce national cyber security status reports, the summary auditing report on the implementation of the cyber security maintenance plan for the government agency, and the national cyber security development programs.
The status report, summary auditing report and the national cyber security development programs of the preceding Paragraph shall be submitted to the Legislative Yuan for review.

Article 6
The competent authority may commission or entrust other government agency, juristic person or organization to implement integrated protection of cyber security, international interchange and cooperation, and other cyber security related issues.
The government agency, juristic person or organization, or re-delegated subcontractor of the preceding Paragraph shall not divulge the secret of critical infrastructure provider which becomes known in the process of enforcement or implement of relevant issues.

Article 7
The competent authority shall stipulate the cyber security responsibility levels by considering the criteria on the importance, confidentiality and sensitivity of the business, the hierarchy of the agency, and the category, quantity and attribute of the information reserved or processed, as well as the scale and attribute of the information and communication system of the government agency and specific non-government agency. The relevant regulations regard the baseline for responsibility levels, application for a change in the level, content of obligation, staffing of dedicated personnel and other regulations and issues concerned shall be stipulated by the competent authority.
The competent authority may audit a specific non-government agency in its implementation of cyber security maintenance plan, of which the frequency, content, method and other issues concerned shall be stipulated by the competent authority.
A specific non-government agency is audited as per preceding Paragraph, and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the competent authority and to the central authority in charge of relevant industry.

Article 8
The competent authority shall set up the cyber security information sharing mechanism.
Regulation regarding analysis, integration, and the sharing of content, procedure and method, and other matters of the cyber security information in the preceding Paragraph shall be stipulated by the competent authority.

Article 9
A government agency or specific non-government agency outsources for setup, maintenance of the Information and communication system, or for provision of Information and communication services, such government agency or specific non-government agency shall, within the realm of this Act, take into account outsourced party's professional capability and experience, as well as nature of the outsourced project and requirement of cyber security, select the appropriate party for outsourcing and oversee its cyber security maintenance service.

Chapter II. Government Agency Cyber Security Management
Article 10
A government agency shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.

Article 11
A government agency shall staff the position of Cyber Security Officer, which to be concurrently served by the deputy head or other appropriate personnel as designated by the agency head. The Cyber Security Officer shall assume the responsibility to carry out and oversee the cyber security business of the agency.

Article 12
A government agency shall submit to the superior or supervisory authority about the implementation of the cyber security maintenance plan annually. Without such superior authority, the implementation report of the cyber security maintenance plan shall be submitted to the competent authority.

Article 13
A government agency shall audit the subordinate authority under its supervision about the implementation of the cyber security maintenance plan.
When an agency is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the auditing agency and the superior or the supervisory authority.

Article 14
To cope with cyber security incident, a government agency shall stipulate the reporting and responding mechanism.
When privy to a cyber security incident, the government agency shall report to the superior or supervisory authority as well as tothe competent authority. Without such superior authority, the government agency shall report to the competent authority.
A government agency shall file a report on the investigation, handling and improvement on the cyber security incident, and shall submit the report to the superior or supervisory authority as well as the competent authority. Without a superior authority, the government agency shall submit to the competent authority.
Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority.

Article 15
Personnel affiliated with government agencies who have excellent performance in maintaining the agency's cyber security shall be incentive awarded.
Regulations for such incentive award in the preceding Paragraph shall be stipulated by the competent authority.

Chapter III. Specific Non-Government Agency Cyber Security Management
Article 16

The central authority in charge of relevant industry shall, after consulting with the relevant government agency, civil associations, scholars and experts for their opinions, designate the critical infrastructure provider and submit to the competent authority for approval, while notifying the approved provider in writing.
A critical infrastructure provider shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.
A critical infrastructure provider shall submit to the central authority in charge of relevant industry about the implementation of the cyber security maintenance plan.
The central authority in charge of relevant industry shall audit the critical infrastructure provider about the implementation of the cyber security maintenance plan.
When a critical infrastructure provider is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the central authority in charge of relevant industry.
Regulations regarding the essentials of the cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in Paragraph 2 to Paragraph 5 shall be drafted by the central authority in charge of relevant industry, and submit to the competent authority for approval.

Article 17
A specific non-government agency other than critical infrastructure provider, shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.
The central authority in charge of relevant industry may request the specific non-government agency under their charge mentioned in the preceding Paragraph, to submit a report about implementation of the cyber security maintenance plan.
The central authority in charge of relevant industry may audit the specific non-government agency under their charge mentioned in the Paragraph 1 regarding their implementation of the cyber security maintenance plan. When found defective or needing improvement in the cyber security maintenance plan, the audited specific non-government agency shall be required to submit an improvement report before a specified date.
Regulations regarding the essentials of the cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in preceding three Paragraphs shall be drafted by the central authority in charge of relevant industry, and submit to the competent authority for approval.

Article 18
To cope with cyber security incident, a specific non-government agency shall stipulate the reporting and responding mechanism.
When privy to a cyber security incident, a specific non-government agency shall report to the central authority in charge of relevant industry.
A specific non-government agency shall file a report on the investigation, handling and improvement on the cyber security incident and shall submit the report to the central authority in charge of relevant industry. In case of a severe cyber security incident, it shall further notify the competent authority.
Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority.
When privy to a severe cyber security incident, the competent authority or

the central authority in charge of relevant industry may, in a timely manner, promulgate the essential contents of the incident and coping measures and render relevant support.

Chapter IV. Penalties
Article 19
Personnel of a government agency shall be subject to discipline or penalty in accordance with the relevant regulations if failing to comply with the regulation of the Act.
Regulations for such penalty in the preceding Paragraph shall be stipulated by the competent authority.

Article 20
If a specific non-government agency has one among those enumerated below transpired, the central authority in charge of relevant industry shall order it to complete corrective actions within the specified time limit. If it fails to complete corrective actions within the specified time limit, it shall be subject to a fine ranging from NT$100,000 as the minimum to NT$1,000,000 as the maximum for each offense:
1. If it fails to stipulate, amend or implement the cyber security maintenance plan in accordance with Paragraph 2 of Article 16 or Paragraph 1 of Article 17, or violates the essential items in the cyber security maintenance plan under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.
2. If it fails to submit the report on implementation of the cyber security maintenance plan to the central authority in charge of relevant industry in accordance with Paragraph 3 of Article 16 or Paragraph 2 of Article 17, or fails the requirements with the submittal of the implementation of the cyber security maintenance plan stipulated under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.
3. If it fails the requirements under Paragraph 3 of Article 7, Paragraph 5 of Article 16 or Paragraph 3 of Article 17, unable to submit the improvement reports to the competent authority, the central authority in charge of relevant industry, or violates the regulation with the submitting of the improvement report under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.
4. If it fails to stipulate the reporting and responding mechanism of cyber security incident in accordance with Paragraph 1 of Article 18, or violates the essential items in the reporting and responding mechanism under Paragraph 4 of Article 18.
5. If it fails the requirements under Paragraph 3 of Article 18, unable to submit the cyber security investigation, handling and improvement reports regarding cyber security incidents to the central authority in charge of relevant industry or the competent authority, or violate the regulation with the submitting of the report under Paragraph 4 of Article 18.
6. If it violates the regulation regarding the contents of notification under Paragraph 4 of Article 18.

Article 21
A specific non-government agency violates the provisions Paragraph 2 of Article 18, by failing to report a cyber security incident, the central authority in charge of relevant industry shall impose a fine ranging from NT$300,000 as the minimum to NT$5,000,000 as the maximum, and shall order it to complete improvement within a specified time limit. If it fails to complete such requirement within the specified time limit, a penalty for each additional offense shall be re-imposed.

Chapter V. Supplementary provisions
Article 22
The enforcement rules of the Act shall be stipulated by the competent authority.

Article 23
The implementation date of the Act shall be stipulated by the competent authority.