Content

Title：	Enforcement Rules of Cyber Security Management Act Ch
Date：	2021.08.23
Legislative：	1.Promulgated on Novenber 21, 2018 2.Amendment promulgated on 23 August 2021
Content：	Article 1 These Rules are stipulated in accordance with Article 22 of the Cyber Security Management Act (hereinafter referred to as the Act). Article 2 The term “military agency” as used in Subparagraph 5 of Article 3 of the Act refers to the Ministry of National Defense and its subordinate agency (institution), troop, school; and the term “intelligence agency” as used therein, refers to the agency specified in Subparagraph 1 of Paragraph 1 and Paragraph 2 of Article 3 of the National Intelligence Services Law. Article 3 In submitting improvement reports under Paragraph 3 of Article 7, Paragraph 2 of Article 13, Paragraph 5 of Article 16 or Paragraph 3 of Article 17 of the Act, the government agency or the specific non-government agency (hereinafter referred to as “each agency”) shall submit the following contents in response to the audit result of the implementation of the cyber security maintenance plan, and shall submit the implementation of the improvement report in the manner and within the time as designated by the competent authority, superior or supervisory authority, the central authority in charge of relevant industry: 1. Flaws or items to be improved. 2. Causes of occurrence. 3. Measures in aspects of management, technology, manpower, or resource to be taken for flaws or items to be improved. 4. The estimated completion schedules of the measures under the preceding subparagraph and the tracking method on implementation progresses. Article 4 When each agency outsources parties for setup, maintenance of information and communication system, or provision of information and communication service (hereinafter referred to as the “outsourced business”) in accordance with Article 9 of the Act, attention should be paid to the following matters for the selection and supervision of the outsourced party. 1. The procedures and environment of the outsourced party in conducting outsourced business shall have completed cyber security management measures or have passed the verification of third party. 2. The outsourced party shall deploy sufficient and properly qualified and trained cyber security professionals who hold cyber security professional licenses or have similar business experience. 3. Whether the outsourced party can second-tier subcontract outsourced business’ scopes and objects that may be second-tier subcontract and the cyber security maintenance measures that the second-tier subcontractor should have. 4. If the outsourced business involves classified national security information, the person who conduct the outsourced business shall be reviewed and the departure shall be controlled in accordance with the Classified National Security Information Protection Act. 5. If the outsourced business includes customized development of information and communication system, the outsourced party shall provide security testing certificate of such information and communication system; if such information and communications system is the core system of the outsourcing agency, or the outsourcing amount exceeds NT$10,000,000, the outsourcing agency shall conduct itself or contract third party to conduct

the security testing; if the use of system or resource other than those developed by the outsourced party is involved, content and source of those not developed by the outsourced party shall be indicated and the certification of authorization thereof shall be provided.
6. If the outsourced party conducts outsourced businesses in violation of the relevant regulatory requirement of cyber security or becomes aware of cyber security incident, it shall immediately notify the outsourcing agency thereof and take remedy measure therefor.
7. If the entrusting relationship is terminated or canceled, it shall be confirmed that the outsourced party has returned, handed over, deleted or destroyed all materials in its possession for the performance of the contract.
8. The outsourced party shall take other relevant measure for cyber security.
9. The outsourcing agency shall, periodically, or whenever it becomes aware of the occurrence of cyber security incident of the outsourced party that might affect the outsourced business, confirm the implementation status of the outsourced business by audit or other appropriate method.
In conducting the competency audit under Subparagraph 4 of the preceding paragraph, the outsourcing agency shall take into consideration the confidential level and content of the classified national security information in which the outsourced business is involved, and shall, to the necessary extent, check whether the personnel of the outsourced party who performs such business or other personnel who might access such classified national security information has any of the following circumstances:
1. One who had committed the offense of disclosing secret, or had committed the offense of civil disturbance or treason after the termination of the Period of National Mobilization in Suppression of Communist Rebellion, and was finally convicted, or was put on a wanted list which has not been closed.
2. One who was aformer public official, was subject to administrative penalty or demerit record due to a violation of relevant regulatory for security confidentiality.
3. One who was induced or coerced by foreign government, mainland China, Hong Kong or Macau government to engage in activity unfavorable to national security or significant interest of the nation.
4. Other concrete item relating to the protection of classified national security information.
The circumstance under Subparagraph 4 of Paragraph 1 shall be stated in the tender notice, tender document and contract; before the verification of the competency audit, the relevant personnel shall agree in writing document.
Article 5
The “inwriting” document under Paragraph 3 of the preceding article and Paragraph 1 of Article 16 of the Act may be the electronic one in accordance with the Electronic Signatures Act.
Article 6
The cyber security maintenance plan under Article 10, Paragraph 2 of Article 16, and Paragraph 1 of Article 17 of the Act shall include the following:
1. Core businesses and their significance.
2. Cyber security policy and objectives.
3. The organization promoting cyber security.
4. The deployment of dedicated manpower and fund.
5. The deployment of Cyber Security Officer of the government agency.
6. The inventory of information and communication systems and information, and indicating the core ones and relevant assets.
7. Risk assessments of cyber security.
8. Protection and control measures for cyber security.
9. The notification, response and rehearsal mechanisms relating to cyber security incidents.
10. Cyber security information assessment and response mechanism.
11. Management measures for outsourced information and communication system or service.
12. Assessment mechanism for personnel of the government agency who conducts business involving cyber security matters.
13. The continual improvement and performance management mechanism for the

cyber security maintenance plan and implementation status.
The implementation of cyber security maintenance plans submitted by each agency under Article 12, Paragraph 3 of Article 16, or Paragraph 2 of Article 17 of the Act shall include the implementation results of and relevant explanations for those under each subparagraph of the preceding paragraph.
The stipulation, amendment, and implementation of the cyber security maintenance plans under Paragraph 1, and the submission of the implementation thereof to be conducted by a government agency may, with consent of its superior or supervisory authority, be conducted by its superior or supervisory authority or another government agency subordinate to its superior or supervisory authority; and in case of a specific non-government agency, the same may, with consent of its central authority in charge of relevant industry, be conducted by its central authority in charge of relevant industry, a subordinate government agency of such central authority in charge of relevant industry, or another specific non-government agency regulated by the central authority in charge of relevant industry.
Article 7
The scope of the core businesses specified in Subparagraph 1 of Paragraph 1 of the preceding article are as follows:
1. Businesses that are considered as the core accountabilities of the government agency as determined by its organizational regulation.
2. Major services or functions of government-owned enterprise and government-endowed foundation.
3. Businesses that are required by each agency for the maintenance and provision of critical infrastructure.
4. Businesses in which each agency is involved in accordance with Paragraphs 1 to 5 of Article 4, or Paragraphs 1 to 5 of Article 5 of the Regulations on Classification of Cyber Security Responsibility Levels.
The term “core information and communication system” as used in Subparagraph 6 of Paragraph 1 of the preceding article refers to the system that is necessary for supporting the continual operation of core business, or that is of high level of defense requirements as determined in accordance with Schedule 9 to the Regulations on Classification of Cyber Security Responsibility Levels - principles of classification of cyber system defense requirement levels.
Article 8
The investigation, handling and improvement report on cyber security incident under Paragraph 3 of Article 14 and Paragraph 3 of Article 18 of the Act shall include the following:
1. Times of the occurrences of or the awareness of the occurrences of the incidents, the completion of damage control or recovery operations.
2. The scope affected by the incidents and the damage assessment.
3. The courses of damage control and recovery operations.
4. The courses of incident investigations and handling operations.
5. Cause analysis of the incident.
6. Measures in aspects of management, technology, manpower or resources taken to prevent the reoccurrences of similar incident.
7. The estimated completion schedule and the follow-up mechanism of the measures under the preceding subparagraph.
Article 9
Before designating critical infrastructure providers under Paragraph 1 of Article 16 of the Act, the central authority in charge of relevant industry shall give such providers the opportunity to state their opinions.
Article 10
The term “severe cyber security incident” as used in Paragraphs 3 and 5 of Article 18 of the Act refer to level-3 and level-4 cyber security incidents specified in Paragraphs 4 and 5 of Article 2 of the Regulations on the Notification and Response of Cyber Security Incidents.
Article 11
When the competent authority or the central authority in charge of relevant industry is privy to a cyber security incident and publicize the necessary contents and countermeasures relating to severe cyber security incidents under Paragraph 5 of Article 18 of the Act, upon awareness of such incidents, times of occurrence or privy of the occurrence, causes,

affection degree, control status, and subsequent improvement measures of such incidents shall be stated in the publications.
Under any of the following circumstances, the necessary contents and contingency measures relating to the incidents under the preceding paragraph shall not be publicized:
1. If it involves trade secrets or information relating to business operations of individuals, juristic persons or organizations or if the disclosure might infringe upon rights or other rightful interests of the government agency, individual, juristic person or organizations; except as is otherwise required by law, or necessary for public welfare or necessary for protection of life, body, and health of people, or with consent of the parties concerned.
2. Other circumstances of confidentiality, restriction, or prohibition on disclosure as required by law.
If the necessary contents and contingency measure relating to the incidents shall not be publicized under Paragraph 1, only the other portion may be publicized.
Article 12
If businesses of the specific non-government agency involve the accountabilities of several central authority in charge of relevant industry, the competent authority may designate via coordination more than one central authority in charge of relevant industry to solely or jointly conduct the matters to be conducted by the central authority in charge of relevant industry under the Act.
Article 13
The implementation date of the Rules shall be stipulated by the competent authority.
The amendments to these Enforcement Rules shall take effect on the date of promulgation.

Data Source：Ministry of Digital Affairs Laws and Regulations Retrieving System