Article Content

Title：	Cyber Security Information Sharing Regulations CH
Amended Date：	2021-08-23
Category：	Executive Yuan (行政院)

Article 1 These Regulations are stipulated in accordance with Paragraph 2 of Article 8 of the Cyber Security Management Act (hereinafter referred to as the Act).

Article 2 The term cyber security information (hereinafter referred to as the Information) as used in these Regulations refers to the information containing any of the following contents:
1. Malicious detections or collections activity of information and communication system.
2. Security vulnerabilities of information and communication system.
3. The methods that invalidate the information and communication systems security control measure or make use of the security vulnerability.
4. The information relating to malicious programs.
5. The actual damage or possible negative impact caused by cyber security incident.
6. Relevant measures that are taken to detect, prevent from or respond to the circumstances under the preceding five subparagraphs or to mitigate the damage.
7. Other technical information relating to cyber security incidents.

Article 3 The competent authority shall conduct international cooperation in the matters of cyber security information sharing.
The competent authority shall timely conduct cyber security information sharing with the government agencies.
The government agency shall timely conduct cyber security information sharing with the competent authority, unless such information has been shared under the preceding paragraph or has been disclosed.
The central authority in charge of relevant industry shall timely conduct cyber security information sharing with the specific non-government agency under their charge.
The specific non-government agency may conduct cyber security information sharing with the central authority in charge of relevant industry.
If the central authority in charge of relevant industry

determines that the cyber security information shared under the preceding paragraph is sufficient to prevent other agency from the occurrence of cyber security incident or to mitigate their damage, the central authority in charge of relevant industry may present incentive award.

Article 4 The cyber security information under any of the following circumstances may not be shared:
1. The information involving business secret or relating to business operation of individual, juristic person or group, of which the disclosure or provision might infringe upon right or other legitimate interest of the government agency, individual, juristic persons or group; unless it is otherwise provided by law, or necessary for public welfare, or necessary for the protection of the lives, bodies or health of the people, or with consent of the party involved.
2. Other circumstances under which cyber security information should be kept confidential, should be restricted on or prohibited from disclosure thereof.
Cyber security information containing contents that may not be shared under the preceding paragraph may be shared to the extent of other portions only.

Article 5 In conducting cyber security information sharing, the government agency or the specific non-government agency (hereinafter referred to as each agency) shall analyze and integrate the information and shall plan the appropriate security maintenance measure to prevent breach of the content of the information, personal information, or information that may not be shared under laws; or the unauthorized access thereto or the tampering thereof.

Article 6 For the cyber security information received, each agency shall identify its reliability and timeliness, shall timely conduct an analysis of threat and vulnerability and make the judgment of potential risk, and shall take corresponding prevention or contingency measure.

Article 7 In conducting cyber security information integration, each agency may conduct the correlation analysis with their internal information based on the source, date of receipt, available periods, and kinds of the information, the extent of threat index, and other proper items.
The government agency may conduct the cyber security sharing of the new threat that is found after the integration.

Article 8 For the cyber security information received, each agency shall take appropriate security measures to prevent the breach of the

content of cyber security information, personal information or information that may not be shared under laws; or the unauthorized access thereto or the tampering thereof.

Article 9 In conducting cyber security information sharing, each agency shall follow the procedure as designated by the competent authority or the central authority in charge of relevant industry, respectively.
If conducting cyber security information sharing in the manner under the preceding paragraph is prevented for any reason, each agency may conduct it in any of the following manners with the consent of the competent authority or the central authority in charge of relevant industry, respectively:
1. Written documents.
2. Fax.
3. Email.
4. Information system.
5. Other appropriate manner.

Article 10 Individual, juristic person or organization, to whom the Act is not applicable, may conduct cyber security information sharing, with the consent of the competent authority or the central authority in charge of relevant industry.
In giving consent to individual, juristic person or organization for cyber security information sharing under the preceding paragraph, the competent authority or the central authority in charge of relevant industry shall agree with them in writing on the provisions of compliance with the requirements under Article 4 to the preceding article.

Article 11 The date for enforcement of these Regulations shall be decided by the competent authority.
The amendments to these Regulations shall take effect on the date of promulgation.