Content

| | |
|---|---|
| Title： | Regulations on the Notification and Response of Cyber Security Incident Ch |
| Date： | 2021.08.23 |
| Legislative： | 1. Promulgated on Novenber 21, 2018<br>2. Amendment promulgated on 23 August 2021 |
| Content： | Chapter 1 General Provisions<br>Article 1<br>These Regulations are stipulated in accordance with Paragraph 4 of Article 14 and Paragraph 4 of Article 18 of the Cyber Security Management Act (hereinafter referred to as the “Act”).<br>Article 2<br>Cyber security incident is classified into four levels.<br>The cyber security incident occurred to the government agency or the specific non-government agency (hereinafter referred to as “each agency”) under any of the following circumstances is the level-1 cyber security incident:<br>1. Minor breach of non-core business information.<br>2. Minor alteration of non-core business information or non-core information and communication system.<br>3. Impact on or interruption of non-core business operation which may be recovered within tolerable interruption time, resulting in impact on daily operation of each agency.<br>The cyber security incident occurred to each agency under any of the following circumstances is the level-2 cyber security incident:<br>1. Serious breach of non-core business information or minor breach of core business information not involving the maintenance and operation of critical infrastructures.<br>2. Serious alteration of non-core business information or non-core information and communication system, or minor alteration of core business information or core information and communication system not involving the maintenance and operation of critical infrastructures.<br>3. Impact on or interruption of non-core business operation, which cannot be recovered within tolerable interruption time, or impact on or interruption of core business or core information and communication system operation not involving the maintenance and operation of critical infrastructures, which may be recovered within tolerable interruption time.<br>The cyber security incident occurred to each agency under any of the following circumstances is the level-3 cyber security incident:<br>1. Serious breach of core business information not involving the maintenance and operation of critical infrastructures, or minor breach of confidential, sensitive information of general official affairs, or minor breach of core business information involving the maintenance and operation of critical infrastructures.<br>2. Serious alteration of core business information or core information and communication system not involving the maintenance and operation of critical infrastructures, or minor alteration of confidential, sensitive information of general official affairs or core business information or core information and communication system involving the maintenance and operation of critical infrastructures.<br>3. Impact on or interruption of the operation of core business or core information and communication system not involving the maintenance and operation of critical infrastructures, which cannot be recovered within the tolerable interruption time, or impact on or interruption of the operation of core business or core information and communication system involving the maintenance and operation of critical infrastructures, which may be recovered within tolerable interruption time.<br>The cyber security incident occurred to each agency under any of the |

following circumstances is the level-4 cyber security incident:
1. Serious breach of confidential, sensitive information of general official affairs or core business information involving the maintenance and operation of critical infrastructures, or the breach of classified national security information.
2. Serious alteration of confidential, sensitive information of general official affairs or core business information or core information and communication system involving the maintenance and operation of critical infrastructures, or the alteration of classified national security information.
3. Impact on or interruption of core business or core information and communication system involving the maintenance and operation of critical infrastructures, which cannot be recovered within tolerable interruption time.

Article 3

Content of the notification of cyber security incident shall include the following items:
1. The agency occurred.
2. The time of occurrence or awareness.
3. The description of the situation.
4. Level assessment.
5. Coping measure in response to the incident.
6. Assessment of requirement for external support.
7. Other relevant items.

Chapter 2 The notification and response of cyber security incident of government agency

Article 4

Upon awareness of the cyber security incident, the government agency shall conduct the notification of the cyber security incident within one hour in the manner and to the objects as designated by the competent authority.
In case of the change to the level of the cyber security incident under the preceding paragraph, the government agency shall continue the notification as provided for in the preceding paragraph.
When the notification conducted in the manner as specified in Paragraph 1 is unavailable for some reason, the government agency shall conduct the notification in another appropriate manner within the timeframes prescribed under the same paragraph, and note the cause of unable notification from being conducted in the required manner.
After eliminating of the cause of unable notification from being conducted in the manner as required under Paragraph 1, the government agency shall supplement the notification in the same manner.

Article 5

After the completion of the notification of the cyber security incident, the competent authority shall complete the review of the level of such cyber security incident within the following timeframes, and may change its level according to the review results:
1. Within eight hours after receipt of the notification of a level-1 or level-2 cyber security incident.
2. Within two hours after receipt of the notification of a level-3 or level-4 cyber security incident.
The Presidential Office, the agencies directly subordinate to the central first-level agencies, and special municipalities and county (city) governments shall, after the notification of the cyber security incident, conducted by themselves, their subordinate or supervisory government agencies, their governed villages (townships/cities), mountain indigenous district offices of special municipalities, and the subordinate or supervisory government agencies of such governed villages (townships/cities) and mountain indigenous district offices of special municipalities, and the representative councils of the above said villages (townships/cities) and Mountain Indigenous Districts of Special Municipalities councils, complete the review of level of such cyber security incident within the timeframes as required under the preceding paragraph, and may change its level according to the review results.
After completion of the required review of the level of the cyber security incident, the agencies under the preceding paragraph shall notify the competent authority of the review results within one hour, and shall

provide information relating to the basis of the reviews.
The Presidential Office, the National Security Council, the Legislative Yuan, the Judicial Yuan, the Examination Yuan, the Control Yuan, and special municipalities and county (city) councils shall, after completion of their own notification of cyber security incident, conduct the review of the level of such cyber security incident within the timeframes as specified under Paragraph 1, and shall notify and provide the competent authority with relevant information as required under the preceding paragraph.
Upon receipt of the notifications under the preceding two paragraphs, the competent authority shall further review the level of the cyber security incident according to the relevant information, and may change its level according to the review result. However, if it is deemed necessary, or if the agencies under Paragraph 2 and the preceding paragraph fail to notify of the required review results, the competent authority may directly review such cyber security incident and may change its level.
Article 6
Upon awareness of the cyber security incident, the government agency shall complete the damage control or recovery operation within the following timeframes, and shall conduct the notification in the manner and to the objects as designated by the competent authority:
1. Within seventy-two hours of the awareness of a level-1 or level-2 cyber security incident;
2. Within thirty-six hours of the awareness of a level-3 or level-4 cyber security incident.
After completion of the damage control or recovery operation under the preceding paragraph, the government agency shall continue the investigation and management of the cyber security incident, and shall submit the investigation, management and improvement report within one month in the manner designated by the competent authority.
The timeframe of submission of the investigation, management, and improvement reports under the preceding paragraph may be extended with the consent of the superior or supervisory authority and the competent authority.
If the superior or supervisory authority or the competent authority deem necessary or deem there is any non-compliance with the regulatory requirement, improper matters or other matters to be improved in respect of the damage control or recovery operation under Paragraph 1 and the report submitted under Paragraph 2, they may require the government agency to give explanations and make adjustments.
Article 7
The Presidential Office, the agencies directly subordinate to central first-level agencies, and the special municipalities and county (city) governments shall provide necessary assistance or support in respect of the notification and response operation of the cyber security incident implemented by the government agency which is subordinate to, or supervised or regulated by, or whose businesses are related to them, if circumstances so require.
The competent authority may provide necessary support and assistance in respect of the response operation of the cyber security incident implemented by the government agency, if circumstances so require.
After the government agency becomes aware of a level-3 or level-4 cyber security incident, its Cyber Security Officer shall convene the meetings to discuss relevant matters, and may request relevant agencies to provide assistances.
Article 8
The Presidential Office, the agencies directly subordinate to central first-level agencies, and the special municipalities and county (city) governments shall plan and conduct cyber security exercise for themselves, their subordinate or supervisory government agencies, their governed villages (townships/cities), mountain indigenous district offices of special municipalities, and the subordinate or supervisory government agencies of such governed villages (townships/cities) and mountain indigenous district offices of special municipalities, and the representative councils of the above said villages (townships/cities) and Mountain Indigenous Districts of Special Municipalities councils, and shall

submit the implementation status thereof and the result reports thereon to the competent authority within one month after the completion thereof.
Content of the exercise operation under the preceding paragraph shall include the following items at least:
1. Social engineering exercise shall be conducted once every six months.
2. The notification and response exercise of the cyber security incident shall be conducted once a year.
The Presidential Office and the central first-level agencies and special municipalities and county/city councils shall plan and conduct the cyber security exercise operation required under the preceding paragraph.
Article 9
The government agency shall stipulate the operational regulations on the notification of the cyber security incident, the content of which shall include the following matters:
1. The process and the accountabilities of judgment and determination of levels of the incident.
2. Assessment of the impact scope and damage degrees of the incident and the response abilities of the agencies.
3. The process of internal notification on the cyber security incident.
4. The method and time of notification to other agencies impacted by the cyber security incident.
5. The exercises under the preceding four paragraphs.
6. The contact window and methods of notification of the cyber security incident.
7. Other matters relating to the cyber security incident.
Article 10
The government agency shall stipulate the operational regulations on the response of the cyber security incident, the content of which shall include the following matters:
1. The organization of the response team.
2. The exercise prior to the occurrence of the incident.
3. The mechanism of damage control on the occurrence of the incident and request for technical support or other necessary assistance from the central authority in charge of relevant industry concerned.
4. Recovery, identification, investigation, and improvement mechanisms after the occurrence of the incident.
5. The preservations of records relating to the incident.
6. Other matters relating to the response of the cyber security incident.
Chapter 3 The notification and response of cyber security incident of the specific non-government agency
Article 11
Upon awareness of the cyber security incident, the specific non-government agency shall conduct the notification of the cyber security incident within one hour in the manner as designated by the central authority in charge of relevant industry.
In case of change to the level of the cyber security incident under the preceding paragraph, the specific non-government agency shall continue the notification as provided for in the preceding paragraph.
If the notification conducted in the manner as specified in Paragraph 1 is prevented for any cause, the specific non-government agency shall conduct the notification in another appropriate manner within the timeframes prescribed under the same paragraph, and note the cause for not being able to report by the prescribed manner.
After the elimination of the cause for preventing the notification from being conducted in the manner as required under Paragraph 1, the specific non-government agency shall supplement the notification in the original manner.
Article 12
After the specific non-government agency has completed the notifications of cyber security incident, the central authority in charge of relevant industry shall complete verification of the level of such cyber security incident within the following timeframes, and may change its level according to the verify results:
1. Within eight hours after receipt of the notification of a level-1 or level-2 cyber security incident.
2. Within two hours after receipt of notification of a level-3 or level-4

cyber security incident.
After completion of the verification of the cyber security incident as required under the preceding paragraph, the central authority in charge of relevant industry shall proceed with the following requirement:
1. If the verification result indicates a level-1 or level-2 cyber security incident, they shall periodically summarize the verification result, basis, and other necessary information, and then submit them to the competent authority in the manner as specified by the competent authority.
2. If the verification result indicates a level-3 or level-4 cyber security incident, they shall, within one hour of the completion of the verification, submit the verification result, basis, and other necessary information to the competent authority in the manner as specified by the competent authority.
Upon receipt of the documentation under the preceding paragraph, the competent authority may review the level of the cyber security incident, and may change its level.
Article 13
Upon awareness of the cyber security incident, the specific non-government agency shall complete damage control or recovery operation within the following timeframes, and shall conduct the notification in the manner as designated by the central authority in charge of relevant industry:
1. Within seventy-two hours of the awareness of a level-1 or level-2 cyber security incident.
2. Within thirty-six hours of the awareness of a level-3 or level-4 cyber security incident.
After completion of damage control or recovery operation under the preceding paragraph, the specific non-government agency shall continue the investigation and management of the cyber security incident, and shall submit the investigation, management, and improvement report within one month in the manner as designated by the central authority in charge of relevant industry.
The timeframe of submission of the investigation, management, and improvement report under the preceding paragraph may be extended with the consent of the central authority in charge of relevant industry.
If the central authority in charge of relevant industry deems necessary or deems there is any non-compliance with regulatory requirement, improper matter or other matter to be improved in respect of the damage control or recovery operation under Paragraph 1 and the report submitted under Paragraph 2, they may require the specific non-government agency to give the explanation and make adjustment.
Upon review of the investigation, management, and improvement report on a level-3 or level-4 cyber security incident submitted by the specific non-government agency, the central authority in charge of relevant industry shall submit such report to the competent authority; if the competent authority deems necessary, or deems there is any non-compliance with regulatory requirement, improper matter, or other matter to be improved, it may require the specific non-government agency to give explanation and make adjustment.
Article 14
The central authority in charge of relevant industry shall provide necessary support or assistance in respect to the notification and response of cyber security incident implemented by the specific non-government agency under its authority, if circumstances so require.
The competent authority may provide necessary support and assistance in respect to the notification and response operation of the cyber security incident implemented by the specific non-government agency, if circumstances so require.
After the specific non-government agency becomes aware of a level-3 or level-4 cyber security incident, it shall convene meetings to discuss relevant matters.
Article 15
The specific non-government agency shall stipulate the operational regulations on the notification of the cyber security incident, the content of which shall include the following matters:
1. The process and the accountabilities of judgment and determination of levels of the incident.

2. Assessment of the impact scope and damage degrees of the incident and the response abilities of the agencies.
3. The process of internal notification on the cyber security incident.
4. The method and time of notification to other agencies impacted by the cyber security incident.
5. The exercises under the preceding four paragraphs.
6. The contact window and methods of notification of the cyber security incident.
7. Other matters relating to the cyber security incident.

Article 16

The specific non-government agency shall stipulate the operational regulations on the response of the cyber security incident, the content of which shall include the following matters:
1. The organization of the response team.
2. The exercise prior to the occurrence of the incident.
3. The mechanism of damage control on the occurrence of the incident and request for technical support or other necessary assistance from the central authority in charge of relevant industry concerned.
4. Recovery, identification, investigation, and improvement mechanisms after the occurrence of the incident.
5. The preservations of records relating to the incident.
6. Other matters relating to the response of the cyber security incident.

Chapter 4 Supplementary Provisions

Article 17

For level-3 or level-4 cyber security incident of each agency, the competent authority may convene meetings and invite relevant agencies to discuss the damage control, recovery, and other relevant matters of such incident.

Article 18

The government agency shall cooperate with the competent authority which shall plan and conduct the cyber security exercise. The content of exercise may include the following matters:
1. Social engineering exercise.
2. The notification and response exercise of the cyber security incident.
3. Cyber offense and defense exercise.
4. Scenario exercise.
5. Other necessary exercise.

Article 19

The specific non-government agency shall, in coordination with the competent authority, plan and conduct the cyber security exercise, the content of which may include the following matters:
1. Cyber offense and defense exercise.
2. Scenario exercise.
3. Other necessary exercise.

If the cyber security exercise planned and conducted by the competent authority has imminent threats of infringement to the rights or legitimate interests of the specific non-government agency, such exercise may be conducted only with written consent of such agency.

The written consent under the preceding paragraph may be made by electronic documents in accordance with the Electronic Signatures Act.

Article 20

If, before the enforcement of these Regulations, the government agency has, independently or jointly with other agencies, formulated the notification and response mechanism for itself or for its subordinate or supervisory government agencies or for its regulated specific non-government agencies, and have enforced such mechanism for more than one year, and maybe approved by the competent authority, they and their subordinate or supervisory government agencies or their regulated specific non-government agencies may continue to conduct the notification and response of cyber security incident according to such mechanism.

In case of change to the notification and response mechanism under the preceding paragraph, such change shall be submitted to the competent authority for approval again.

Article 21

The implementation date of these Regulations shall be stipulated by the competent authority.

| | |
|---|---|
| | The amendments to these Regulations shall take effect on the date of promulgation. |