Content

Title：	Regulations Governing the Reporting, Response and Drills for Cyber Security Incidents Ch
Date：	2026.01.05
Legislative：	1.On November 21, 2018, the Executive Yuan issued Order yuan tai hu zi No. 1070213547, promulgating 21 articles in full; the date those provisions come into effect will be set by the competent authority On December 5, 2018, the Order yuan tai hu zi No. 1070217128 promulgated by the Executive Yuan effective on January 1, 2019 2.On August 23, 2021, the Executive Yuan issued Order yuan tai hu zi No. 1100182012, amending Articles 6, 13 and 21; the amendments come into effect on the date of issuance On August 24, 2022, the Executive Yuan announced yuan tai gui zi No. 1110184307 that the duties listed under the “Executive Yuan” in Paragraph 1 of Article 4, Paragraphs 1, 3, 4, 5 of Article 5, Article 6, Paragraph 2 of Article 7, Paragraph 1 of Article 8, Paragraphs 2, 3 of Article 12, Paragraph 5 of Article 13, Paragraph 2 of Article 14, Article 17, Article 18, Paragraphs 1, 2 of Article 19, Article 20, Paragraph 1 of Article 21 will be transferred to the “Ministry of Digital Affairs”, effective on August 27, 2022. However, Paragraph 1 of Article 5, concerning the Executive Yuan’s review and adjustment of its own cyber security responsibility level remains under the jurisdiction of the “Executive Yuan” 3.On January 5, 2026, the Ministry of Digital Affairs issued Order shu shou zi fa zi No. 1145000415, amending and publishing the title and full text of 20 articles, the amendments come into effect on the date of issuance (Former name: Regulations on the Notification and Response of Cyber Security Incident; New name: Regulations Governing the Reporting, Response, and Drills of Cyber Security Incidents)
Content：	Chapter I. General Provisions Article 1 These Regulations are prescribed pursuant to Paragraph 4, Article 10; Paragraph 4, Article 17; and Paragraph 4, Article 24 of the Cyber Security Management Act (hereinafter referred to as the “Act”). Article 2 Cyber security incidents are classified into four levels. A cyber security incident occurring at a government agency or a specific non-government agency (hereinafter referred to as an “agency”) under any of the following circumstances is a level 1 cyber security incident: 1. Minor disclosure of non-core business information. 2. Minor tampering with non-core business information or a non-core information and communication system. 3. The operation of a non-core information and communication system is affected or interrupted, but can be restored within the tolerable interruption time, thereby affecting the agency’s routine operations. A cyber security incident occurring at an agency under any of the following circumstances is a level 2 cyber security incident: 1. Serious disclosure of non-core business information, or a minor disclosure of core business information not involving the maintenance or operation of critical infrastructure. 2. Serious tampering with non-core business information or a non-core information and communication system, or minor tampering with core business information or a core information and communication system not involving the maintenance or operation of critical infrastructure.

3. The operation of a non-core information and communication system is affected or interrupted and cannot be restored within the tolerable interruption time, or the operation of a core information and communication system not involving the maintenance or operation of critical infrastructure is affected or interrupted but can be restored within the tolerable interruption time.

A cyber security incident occurring at an agency under any of the following circumstances is a level 3 cyber security incident:

1. Serious disclosure of core business information not involving the maintenance or operation of critical infrastructure, or a minor disclosure of confidential information relating to general official affairs or of core business information involving the maintenance or operation of critical infrastructure.
2. Serious tampering with core business information or a core information and communication system not involving the maintenance or operation of critical infrastructure, or minor tampering with confidential information relating to general official affairs, core business information, or a core information and communication system involving the maintenance or operation of critical infrastructure.
3. The operation of a core information and communication system not involving the maintenance or operation of critical infrastructure is affected or interrupted and cannot be restored within the tolerable interruption time, or the operation of a core information and communication system involving the maintenance or operation of critical infrastructure is affected or interrupted but can be restored within the tolerable interruption time.

A cyber security incident occurring at an agency under any of the following circumstances is a level 4 cyber security incident:

1. Serious disclosure of confidential information relating to general official affairs, or of core business information involving the maintenance or operation of critical infrastructure, or a disclosure of classified national security information.
2. Serious tampering with confidential information relating to general official affairs, core business information, or a core information and communication system involving the maintenance or operation of critical infrastructure, or tampering with classified national security information.
3. The operation of a core information and communication system involving the maintenance or operation of critical infrastructure is affected or interrupted and cannot be restored within the tolerable interruption time.

Article 3

The reporting of cyber security incidents shall include the following information:

1. The affected agency.
2. The time of occurrence or awareness.
3. A description of the incident.
4. The incident level assessment.
5. Countermeasures for the incident.
6. Assessment of the need for external support.
7. Other relevant matters.

Article 4

Each agency shall stipulate operational guidelines for the reporting of cyber security incidents, which shall include the following matters:

1. The process and responsibility for the determination of incident levels.
2. Assessment of the scope of impact, the extent of damage, and the agency's response capabilities.
3. Internal reporting procedures for cyber security incidents.
4. Methods for notifying other agencies affected by the cyber security incident.
5. Drills covering the matters set out in the preceding four subparagraphs.
6. The reporting point of contact and contact methods for cyber security incident reporting.
7. Other matters relating to the reporting of cyber security incidents.

Article 5

Each agency shall stipulate operational guidelines for the response to cyber security incidents, the content of which shall include the following matters:
1. The organization of the response team.
2. Drills to be conducted before an incident occurs.
3. Damage-control mechanisms upon the occurrence of an incident.
4. Recovery, identification, investigation, and corrective mechanisms after an incident occurs.
5. Preservation of records relating to the incident.
6. Other matters relating to the response of cyber security incidents.

Chapter II. Reporting, Response and Drills of Cyber Security Incidents of Government Agencies

Article 6

A government agency shall, within one hour after becoming aware of a cyber security incident, report the matter on the system platform designated by the competent authority.

Where the level of the cyber security incident changes under the preceding paragraph, the government agency shall continue to update the report in accordance with the preceding paragraph.

Where reporting cannot be made in the manner specified in Paragraph 1 for any reason, the government agency shall report in another appropriate manner within the prescribed timeframe and state the reason why it was unable to report in the prescribed manner.

After the reason for being unable to report in the manner required under Paragraph 1 has been eliminated, the government agency shall report the matter retroactively in the prescribed manner.

Article 7

The agency notified pursuant to Paragraph 2, Article 17 of the Act shall, after receiving a report of a cyber security incident, complete its review of the incident level within the following timeframes and may change the level based on the review results:

1. Within eight hours after receipt of a report of a level 1 or level 2 cyber security incident.
2. Within two hours after receipt of a report of a major cyber security incident.

After completing the review under the preceding paragraph, the notified agency shall, within one hour, notify the competent authority of the review results and provide information on the basis for the review.

Upon receipt of the notification under the preceding paragraph, the competent authority shall further review the incident level based on the relevant information and may change the level based on the review results. However, where it deems it necessary, or where the notified agency fails to notify the review results as required, the competent authority may directly review the cyber security incident and change its level.

Article 8

Upon becoming aware of a cyber security incident, a government agency shall, within the following timeframes, complete damage-control or recovery operations and notify the notified agency under Paragraph 2, Article 17 of the Act in the manner designated by the competent authority:

1. Within 72 hours after becoming aware of a level 1 or level 2 cyber security incident.
2. Within 36 hours after becoming aware of a major cyber security incident.

After completion of the damage control or recovery operations under the preceding paragraph, the government agency shall continue the investigation and handling of the cyber security incident, and shall submit the investigation, handling, and corrective action report on the cyber security incident to the notified agency referred to in the preceding paragraph within one month, in the manner designated by the competent authority.

The timeframe for submission of the investigation, handling, and corrective action report under the preceding paragraph may be extended with the consent of the notified agency referred to in Paragraph 1.

The investigation, handling, and corrective action report referred to in Paragraph 2 shall include the matters specified in Article 12 of the

Enforcement Rules of the Act.
Where the notified agency referred to in Paragraph 1 deems it necessary, or finds any violation of laws or regulations, impropriety, or other matter requiring improvement in the damage-control or recovery operations under the same paragraph or in the report submitted under Paragraph 2, it may require the government agency to provide explanations and make adjustments.

Article 9
The agency notified pursuant to Paragraph 2, Article 17 of the Act shall, as circumstances require, provide necessary support or assistance with respect to the reporting and response operations for cyber security incidents carried out by its subordinate or supervised government agencies, and the following entities under its jurisdiction: township (town, city) offices, district offices of indigenous districts in special municipalities, township (town, city) representative councils, and representative councils of indigenous districts in special municipalities.
The competent authority shall, as circumstances require, provide necessary support or assistance for the response operations for cyber security incidents carried out by government agencies.
After a government agency becomes aware of a major cyber security incident, its Chief Information Security Officer shall convene a meeting to discuss relevant matters and may request relevant agencies to provide assistance.

Article 10
The directly affiliated agencies of the Office of the President, the National Security Council, and the Five Yuans shall plan and carry out cyber security drills for themselves or for their subordinate or supervised government agencies. Within one month after the drills are completed, they shall submit a report on their implementation and results to the competent authority. The drills shall include at least the following items:
1. Social engineering drills shall be conducted once every six months.
2. Reporting and response drills for cyber security incidents shall be conducted once every year.
The Office of the President, the National Security Council, the Five Yuans, and special municipality and county/city councils shall plan and conduct the cyber security drill operations referred to in the preceding paragraph.
Special municipality and county/city governments shall, in accordance with Paragraph 1, plan and carry out cyber security drills for themselves or their subordinate or supervised government agencies, as well as the following agencies:
1. The township (town, city) offices and district offices of indigenous districts in special municipalities under their jurisdiction, and their subordinate or supervised government agencies.
2. The representative councils of townships (towns, cities) and indigenous districts of special municipalities referred to in the preceding subparagraph.

Chapter III. Reporting and Response of Cyber Security Incidents by Specific Non-Government Agencies
Article 11
A specific non-government agency shall, within one hour after becoming aware of a cyber security incident, report the matter in the manner designated by the central competent authority in charge of the relevant sector.
Where the level of the cyber security incident changes under the preceding paragraph, the specific non-government agency shall continue to update the report in accordance with the preceding paragraph.
Where reporting cannot be made in the manner specified in Paragraph 1 for any reason, the specific non-government agency shall report in another appropriate manner within the prescribed timeframe and state the reason why it was unable to report in the prescribed manner.
After the reason for being unable to report in the manner required under Paragraph 1 has been eliminated, the specific non-government agency shall report the matter retroactively in the prescribed manner.

Article 12

After a specific non-government agency has completed reporting of a cyber security incident, the central competent authority in charge of the relevant sector shall complete its review of the incident level within the following timeframes, and may change the level based on the review results:
1. Within eight hours after receipt of a report of a level 1 or level 2 cyber security incident.
2. Within two hours after receipt of a report of a major cyber security incident.
After completing the review under the preceding paragraph, the central competent authority in charge of the relevant sector shall, within one hour, submit the review results, the basis for the review, and other necessary information to the competent authority in the manner specified by the competent authority.
Upon receipt of the information under the preceding paragraph, the competent authority may review the incident level and change it accordingly. However, where it deems it necessary, or where the central competent authority in charge of the relevant sector fails to report the review results as required, the competent authority may directly review the cyber security incident and change its level.

Article 13
Upon becoming aware of a cyber security incident, a specific non-government agency shall, within the following timeframes, complete damage-control or recovery operations and notify in the manner prescribed by the central competent authority in charge of the relevant sector:
1. Within 72 hours after becoming aware of a level 1 or level 2 cyber security incident.
2. Within 36 hours after becoming aware of a major cyber security incident.
After completing the damage-control or recovery operations under the preceding paragraph, the specific non-government agency shall continue the investigation and handling of the cyber security incident and shall submit an investigation, handling, and corrective action report within one month in the manner designated by the central competent authority in charge of the relevant sector.
The timeframe for submission of the investigation, handling, and corrective action report under the preceding paragraph may be extended with the consent of the central competent authority in charge of the relevant sector.
The investigation, handling, and corrective action report referred to in Paragraph 2 shall include the matters specified in Article 12 of the Enforcement Rules of the Act.
Where the central competent authority in charge of the relevant sector deems it necessary, or finds any non-compliance with regulatory requirements, impropriety, or other matter requiring correction in the damage-control or recovery operations under Paragraph 1 or in the report submitted under Paragraph 2, it may require the specific non-government agency to provide explanations and make adjustments.
Upon reviewing the investigation, handling, and corrective action report on a major cyber security incident submitted by the specific non-government agency, the central competent authority in charge of the relevant sector shall submit the report to the competent authority. Where the competent authority deems it necessary, or finds any non-compliance with regulatory requirements, impropriety, or other matter requiring correction, it may require the specific non-government agency to provide explanations and make adjustments.

Article 14
The central competent authority in charge of the relevant sector shall, as circumstances require, provide necessary support or assistance with respect to the reporting and response operations for cyber security incidents carried out by the specific non-government agencies under its jurisdiction.
The competent authority shall, as circumstances require, provide necessary support or assistance for the response operations for cyber security incidents carried out by specific non-government agencies.
After a specific non-government agency becomes aware of a major cyber security incident, its Chief Information Security Officer shall convene a

meeting to discuss relevant matters and may request relevant agencies to provide assistance.

Chapter IV. Supplementary Provisions
Article 15
For cyber security incidents affecting agencies, the competent authority may convene meetings based on the scope of impact and the extent of damage, and invite relevant agencies to discuss damage control, recovery, and other related matters in connection with the incident.

Article 16
Under Paragraph 2, Article 17 of the Act, government agencies shall cooperate with cyber security drill operations planned or conducted by the notified agency, the contents of which may include the following matters:
1. Social engineering drills.
2. Reporting and response drills for cyber security incidents.
3. Cyber offense and defense drills.
4. Scenario-based drills.
5. Other necessary drills.
Under the preceding paragraph, specific non-government agencies shall cooperate with cyber security drill operations planned or conducted by the central competent authority in charge of the relevant sector. However, where such a drill may infringe upon the rights or legitimate interests of a specific non-government agency, it may be conducted only with the agency's prior written consent.
Where cyber security drill operations planned and conducted by the competent authority under Paragraph 4, Article 10 of the Act may infringe upon the rights or legitimate interests of a specific non-government agency, such drill operations may be conducted only with the agency's prior written consent.

Article 17
For all cyber security drill operations planned and conducted in accordance with the preceding article, any participant who becomes aware of confidential or sensitive information of a government agency or a specific non-government agency during the course of the drills shall keep such information confidential.

Article 18
If, before these Regulations enter into force, a government agency has, independently or jointly with other agencies, formulated a reporting and response mechanism for itself, its subordinate or supervised government agencies, or the specific non-government agencies under its jurisdiction, and has implemented such mechanism for one year or more, the agency, along with its subordinate or supervised government agencies or the specific non-government agencies under its jurisdiction, may, upon approval by the competent authority, continue to handle the reporting and response of cyber security incidents in accordance with such mechanism.
Where the reporting and response mechanism referred to in the preceding paragraph is amended, the amendment shall be resubmitted to the competent authority for approval.

Article 19
The competent authority may delegate matters relating to the reporting, response, and drills for cyber security incidents, as well as other related tasks set out in these Regulations, to the Administration for Cyber Security, Ministry of Digital Affairs.

Article 20
These Regulations shall come into effect on the date of promulgation.

Files： 資通安全事件通報應變及演練辦法.pdf