Content

Title：	Administration Regulations of Cyber Security on Telecommunications Business Ch
Date：	2020.07.09
Legislative：	1.14 Articles in full enacted and promulgated by National Communications Commission (NCC) on July 9, 2020. Ref：Tung-Chuan-Ji-Chu Tze No. 10963016330
Content：	Article 1 These Regulations are enacted in accordance with Paragraph 3, Article 15 of Telecommunications Management Act (hereinafter referred to as the Act). Matters not provided herein shall be subject to provisions under other relevant laws and regulations Article 2 Telecommunications enterprises that have established a public switched telecommunications network (PSTN) using telecommunications resources or other telecommunications enterprises (hereinafter referred to as telecommunications enterprises), as announced by the competent authority, shall establish a cyber (info-communications) security maintenance plan in accordance with Paragraph 2, Article 15 of the Act. When making the announcement specified in the preceding paragraph, the competent authority shall take full consideration of the following: 1. Critical telecommunications infrastructure; 2. Whether the number of users or network has reached a specific scale that can result in significant influence, or whether it is deemed necessary due to management of control or other factors; 3. Whether a relevant agency has provided a warning of potential harm to national or information security; 4. Whether a cyber-security incident that occurred has reached level 3 as specified in Regulations on the Notification and Response of Cyber Security Incident. Article 3 The telecommunications enterprises shall, within three months upon receipt of the competent authority's notification, establish the cyber security maintenance plan; submit it to the competent authority for reference; and implement the plan accordingly. Where the cyber security maintenance plan submitted by the telecommunications enterprise as described in the preceding paragraph is deemed incomplete, a revised plan shall be submitted accordingly within the duration prescribed by the competent authority. The management scope of the cyber security maintenance plan specified in Paragraph 1 shall include at least the following items: 1. Equipment and functional devices of the telecommunications network, telecommunications equipment room and network management center; 2. PSTN maintenance systems, including the operations maintenance system and business maintenance system. The operations maintenance system shall include core network and access network systems, whereas the business maintenance system shall include user data, customer services and accounting systems; 3. Cyber security protection facilities established to protect those specified in the preceding two subparagraphs. With respect to the information and communications technology (ICT) system protection and classification methods of the cyber security maintenance plan specified in Paragraph 1, telecommunications enterprises shall comply with the protection levels and classification methods announced by the competent authority. Article 4 Telecommunications enterprises shall, within two years upon the provision

of telecommunications services, successfully obtain the following cyber security management compliant verification standards and maintain the validity thereof accordingly:
1. CNS 27001 national standards or ISO/IEC 27001 international standards;
2. The Additional ISO/IEC 27011 Audit List of the Cyber Security Management Manual for Telecommunications Enterprises.
The scope of the verification specified in the preceding paragraph shall be reported to the competent authority prior to the verification for approval. The same rule shall apply to any amendment subsequently made.
Where any of the following circumstances occurs, the telecommunications enterprise shall propose amendments to the scope of verification upon notification of the competent authority; and shall successfully obtain the cyber security management compliant verification within the period prescribed by the competent authority:
1. Where a cyber security incident that occurred has reached level 3 as specified in Regulations on the Notification and Response of Cyber Security Incident;
2. Where a relevant agency has provided a warning of potential harm to national or information security;
The competent authority may require the telecommunications enterprises to reduce the duration specified in Paragraph 1 upon notification from the national security or cyber security related agency.
Article 5
The following matters shall be specified for the implementation of cyber security maintenance plan for telecommunications enterprises:
1. Cyber security policy and objectives;
2. Core businesses and their significance;
3. The cyber security maintenance scope of PSTN;
4. The organization promoting cyber security;
5. The inventory plan for information and cyber systems;
6. Risk assessments of cyber security;
7. Protection and control measures for cyber security;
8. The continual improvement and performance management mechanism for the cyber security maintenance plan and implementation status.
Where the telecommunications enterprise specified in the preceding paragraph is designated by the competent authority as the provider of critical infrastructure, not only matters in subparagraphs of the preceding paragraph shall be specified in its implementation of the cyber security maintenance plan, but also the following matters:
1. The deployment of dedicated manpower and funds;
2. The deployment of the Cyber Security Officer;
3. Cyber security incident notification, response and drill related mechanism;
4. Cyber security information assessment and response mechanism;
5. Management measures for outsourced information and communications system or service;
6. Assessment mechanism for personnel conducting business involving cyber security matters;
7. Plan for the establishment and implementation of the cyber security detection and protection;
8. Measures to be undertaken with regards to the security protection of user privacy and user data compiled, stored, processed and used during the implementation of the plan specified in the preceding subparagraph;
9. The plan of implementation that has been verified as cyber security management.
Article 6
Telecommunications enterprises shall establish cyber security incident notification, handling, reporting and joint defense measures.
Upon the occurrence of a cyber security incident, telecommunications enterprises shall conduct emergency response measures according to the cyber security incident notified by the competent authority; and shall report the implementation thereof to the competent authority. Relevant records shall be retained for at least six months.
Response measures for telecommunications enterprises designated as the critical infrastructure provider shall be conducted in accordance with Regulations on the Notification and Response of Cyber Security Incident

enacted according to Paragraph 4 of Article 18 of Cyber Security Management Act.

Article 7

Where any amendment is made to the cyber security maintenance plan, telecommunications enterprises shall specify the reason(s) and report it to the competent authority.

Where the plan specified in the preceding paragraph is deemed incomplete, the telecommunications enterprise shall revise the plan within the duration prescribed by the competent authority.

Article 8

The telecommunications equipment room of telecommunications enterprises shall be established in a physical isolation and be equipped with an independent entrance and exit.

The access control security management systems, including all-weather intrusion alerts and video surveillance, shall be installed at the entrance and exit specified in the preceding paragraph. The alerts and recorded videos shall be retained for at least six months.

The telecommunications equipment room specified in Paragraph 1 shall only be accessed by those with purposes of installation, maintenance, monitoring or other operational purposes deemed necessary.

Telecommunications enterprises shall determine their respective security management and operation rules for telecommunications equipment rooms.

The security management and operation rules as described in the preceding paragraph shall include at least the following items:

1. Division of authority: including authorities related to the security maintenance zone, responsible units, staff organization and duties, and access to the telecommunications equipment room;
2. Access control management: including the identification(name and ID card or passport number), organization(institution) entry(exit) time and entry(exit) purposes of the persons entering and leaving the machine room; auditor's audit records; and objects entering(leaving) the room;
3. Maintenance management: management of the maintenance works conducted by internal staff or subcontractors.
4. Environment management: management of fire-fighting, security, electricity and relevant facilities.
5. Management records: including the access management, maintenance management and environment maintenance records.
6. Audit(s): regular and irregular audit works.

The management records specified in Subparagraph 5 of the preceding paragraph shall be retained for at least six months.

With respect to the security management and operation rules for telecommunications equipment rooms specified in Paragraph 4, the competent authority may require the telecommunications enterprise to make amendments according to the implementation status thereof.

The telecommunications enterprise shall implement the security management and operation rules for telecommunications equipment rooms specified in Paragraph 4; the competent authority may conduct an inspection on a regular basis or when deemed necessary.

Article 9

With respect to persons who can potentially harm national security, the national security or cyber security relevant agency shall notify the competent authority thereof. Upon receipt of the competent authority's notification, the telecommunications enterprise shall prohibit the said person from entering the telecommunications equipment room.

Article 10

Where the cyber system software or maintenance system outsourced by the telecommunications enterprise for design or establishment is related to network system resources and users' personal data and communication, the telecommunications enterprise shall notify the competent authority thereof in advance. The maintenance and operations works thereof shall be supervised by the personnel of the telecommunications equipment room throughout the process; all system connection instructions shall be fully recorded; and relevant records shall be retained for at least six months.

Telecommunications enterprise shall not entrust any person(s) who can potentially harm the national security to establish or design the software of the cyber system relating to network system resources and users'

personal data and communication; or to maintain, operate and test the connection of remote systems.

Article 11

Telecommunications enterprises that have been notified of an impending inspection by the competent authority shall, prior to the audit date, prepare a report on the implementation of the cyber security maintenance plan. The said report and supporting evidence therefor shall be provided to the competent authority during the on-site inspection.

Telecommunications enterprises that are unable to accept the inspection as described in preceding paragraph or accept the inspection on the designated audit date shall specify the reason(s) in writing and submit it to the competent authority within five days upon receipt of the notification specified in the preceding paragraph.

The application specified in the preceding paragraph shall be limited to one time only except for cases of force majeure.

Prior to the on-site inspection specified in Paragraph 1, the competent authority may conduct interviews with personnel of the telecommunications enterprise.

Article 12

In order to conduct the inspection specified in Paragraph 1 of the preceding article, the competent authority shall form an inspection team.

The inspection team specified in the preceding paragraph shall consist of three to seven individuals, serving as representatives of official agencies or experts and scholars who have the technical, management, legal or practical expertise and knowledge required for the cyber security policy or the inspection. The representatives of official agencies shall not be less than one third of the total number of inspectors.

Any representative of official agencies or experts and scholars specified in the preceding paragraph shall voluntarily recuse themselves from serving as members of the inspection team in any of the following circumstances:

1. The person, the spouse, the relatives or family members within the third degree of kinship, or trustees of the property trust of the aforementioned people, have a property or non-property interest relationship with the audited special non-official agency or its responsible person.
2. The person, the spouse, and the relatives or family members within the third degree of kinship, have employment, contract, appointment, agent or other similar relationship with the audited special non-official agency or its responsible person at present or within the previous two years.
3. At present or in the previous two years, the person has provided consultancy or counseling to the audited special non-official agency on the matters related to the audited items.
4. Other circumstances that are deemed to be sufficient for the serving as members of the inspection team to affect the impartiality of the audit results.

The competent authority shall reach an agreement with the members of the inspection team in writing on the recusal matters due to conflicts of interest and the confidentiality obligations of executing audit.

Article 13

If the implementation of the telecommunications enterprise's cyber security maintenance plan specifies deficiencies or pending corrective action to be undertaken following the inspection, a report of corrective action shall be submitted to the competent authority within one month after receiving the results of the inspection.

Upon submission of the report of corrective action mentioned in the preceding paragraph, the inspected telecommunications enterprise shall submit an implementation improvement report according to the methods and time designated by the competent authority. If deemed necessary, the competent authority may require the telecommunications enterprise to explain or improve the said report.

Article 14

These Regulations shall take effect on July 1, 2020.