Content

Title：	Regulations on Classification of Cyber Security Responsibility Levels Ch
Date：	2022.08.23
Legislative：	1. Promulgated on Novenber 21, 2018 2. Amendment promulgated on 26 August 2019 3. Amendment promulgated on 23 August 2021
Content：	Article 1 These Regulations are stipulated according to Paragraph 1 of Article 7 of the Cyber Security Management Act (hereinafter referred to as “the Act”). Article 2 The cyber security responsibility levels of the government agency or specific non-government agency(hereinafter referred to as “each agency”) are classified from high to low into Level-A, Level-B, Level-C, Level-D and Level-E. Article 3 The competent authority shall approve its own cyber security responsibility levels every two years. The agencies directly subordinate to the Executive Yuan shall, every two years, propose the cyber security responsibility levels of their own, their subordinate or supervisory government agencies, and the specific non-government agencies under their charge, and shall report the same to the competent authority for approval. Special municipality, county (city) governments shall, every two years, propose the cyber security responsibility levels of their own, their subordinate or supervisory government agencies, and their governed villages (townships/cities), mountain indigenous district offices of municipality, and the subordinate or supervisory government agencies of such governed villages (townships/cities) and mountain indigenous district offices of special municipalities, and shall report the same to the competent authority for approval. Special municipality and county (city) councils, village (township/city) councils, and mountain indigenous districts of special municipality councils shall, every two years, submit their own cyber security responsibility levels, which shall be compiled and submitted by the municipality and county (city) governments where they are located to the competent authority for approval. The Presidential Office, the National Security Council, the Legislative Yuan, the Judicial Yuan, the Examination Yuan, and the Control Yuan shall, every two years, approve the cyber security responsibility levels of their own, their subordinate or supervisory government agencies, and the specific non-government agencies under their charge, and shall submit the same to the competent authority for recordation. If each agency is required to change its cyber security responsibility levels due to adjustments to organizations or businesses, it shall immediately conduct the change to levels according to the procedures under the preceding five paragraphs; the same shall apply to the case when a new agency is established. In conducting the submission or approval of cyber security responsibility levels under Paragraph 1 to Paragraph 5, if the government agency thinks it is necessary to otherwise give the entities within the government agency or the specific non-government agency the levels that are different from those of such agency, it may determine such levels in accordance with the requirements of Article 4 to Article 10, by taking into consideration the nature of businesses of such entities. Article 4 The cyber security responsibility levels of each agency under any of the following circumstances are Level-A:

1. Its business involves classified national security information.
2. Its business involves matters of foreign affairs, national defense, or homeland security.
3. Its business involves the maintenance operation of information and communication system commonly used for nationwide people services or cross agencies.
4. Its business involves the possession of personal information of nationwide people or public officials.
5. It is a government agency, and its business involves matters of nationwide critical infrastructure.
6. It is a critical infrastructure provider, and the central government level authority in charge of the subject industry, based on the consideration of the number of users, market share, the area and the substitutability of its business or maintenance operation of critical infrastructures and services, considers that the failures of or impact on its cyber security system might cause disasters or extremely serious impact on social public interests, people's morale, or the security of people's lives, body or property.
7. It is a government medical center.

Article 5

The cyber security responsibility levels of each agency under any of the following circumstances are Level-B.
1. Its business involves the security maintenance and management of national core technology information that is donated, funded, researched, or developed by the government agency.
2. Its business involves the maintenance operation of information and communication systems that are commonly used for regional or local people services or cross agencies.
3. Its business involves the possession of the archives of personal information of regional or local people.
4. Its business involves the maintenance operation of information and communication systems that are commonly used for the central secondary authority and its subordinate government agencies (institutions).
5. It is a government agency, and its business involves matters of regional or local critical infrastructure.
6. It is a critical infrastructure provider, and the central authority in charge of relevant industry, based on consideration of the number of users, market share, the area and the substitutability of its business, or the maintenance operation of critical infrastructure and services, considers that the failure of or impacts on its information and communication system might cause serious impact on social public interest, people's morale, or the security of people's lives, body or properties.
7. It is a public regional hospital or local hospital.

Article 6

The cyber security responsibility levels of each agency who maintains and operates by itself or outsources the establishment and development of cyber systems are Level-C.

The information and communication system established by itself or outsourced under the preceding paragraph, refers to the information and communication system with authority-division and management functions.

Article 7

The cyber security responsibility levels of each agency who conducts information and communication business by itself but does not maintain and operate the information and communication system that is established and developed by itself or outsourced for the development thereof are Level-D.

Article 8

The cyber security responsibility levels of each agency under any of the following circumstances are Level-E:
1. It neither has the information and communication system, nor provides the information and communication service.
2. It is a government agency, and all its information and communication business is conducted concurrently or managed by its superior agency, supervisory agency or the agency designated by the agencies mentioned above.
3. It is a specific non-government agency, and all of its information and communication business is conducted concurrently or managed by its central

authority in charge of relevant industry, the subordinate government agency of the central authority in charge of relevant industry, the specific non-government agency under their charge by the central authority in charge of relevant industry, or the funding government agency.

Article 9

If the cyber security responsibility levels of each agency conforms to two or above requirements under Article 4 to the preceding articles, the levels of such agency are classified as the highest level conforming to such requirements.

Article 10

The cyber security responsibility levels of each agency shall be determined in accordance with the preceding six articles; however, when the government agency submits or approves the cyber security responsibility levels under Paragraphs 1 to 5 of Article 3, the levels of each agency may be adjusted, by taking into consideration the degree of impact of the following matters on national security, social public interests, the security of people’s lives, body, or properties, or the reputation of the government agency:

1. If its business involves foreign affairs, national defense, homeland security, or its business involves nationwide, regional or local energy, water resources, telecommunication, transportation, banking & finance, emergent rescues, and hospitals.
2. If its business involves personal information, official confidentiality, or other information which should be confidential by law or by contract - the quantity and nature of such information, and the unauthorized access, use, control, breach, damage, tampering, destruction or other infringement.
3. Depending on different levels of each agency - the impact on, failure, or interruption of its functions.
4. Other concrete matters relating to the provision, maintenance operation, size, or nature of information and communication system.

Article 11

Each agency shall conduct the matters specified in Schedule 1 to Schedule 8, depending on its cyber security responsibility levels.

For the information and communication system that is developed by each agency itself or outsourced for the development, each agency shall complete the classification of information and communication system according to the principles of classification of defense requirements of information and communication system specified in Schedule 9, and shall implement control measures according to the defense standards of information and communication system specified in Schedule 10; if the central authority in charge of relevant industry of a specific non-government agency considers it is necessary to otherwise provide for defense standards of specific types of the information and communication systems, it may propose by itself the defense standards and report such standards to the competent authority for approval, and shall follow the requirements of such standards, if approved.

In conducting the matters specified in Schedule 1 to Schedule 8 or implementing control measures specified in Schedule 10, if each agency has apparent difficulties in conducting or implementing specific matters or control measures due to such factors as technical limitation, design, structure or nature of individual cyber systems, it may, with consent of each agency submitting its levels under Paragraph 2 to Paragraph 4 of Article 3 or each agency approving its levels under Paragraph 5 of the same article, and upon reporting to the competent authority for recordation, be exempted from the implementation of such matters or control measures.

The government agency whose cyber security responsibility levels are Level-A or Level-B shall report the implementation status of matters under Paragraph 1 and Paragraph 2 in the manner designated by the competent authority.

The central authority in charge of relevant industry may require the specific non-government agency regulated under their charge to report the implementation status of matters under Paragraph 1 and Paragraph 2 in the manner designated.

Schedule 1：Matters to be conducted by the government agency of cyber security responsibility Level-A.pdf

Schedule 1：Matters to be conducted by the government agency of cyber security responsibility Level-A.doc

Schedule 2：Matters to be conducted by the specific non-government agency of cyber security responsibility Level-A.pdf
Schedule 2：Matters to be conducted by the specific non-government agency of cyber security responsibility Level-A.doc
Schedule 3：Matters to be conducted by the government agency of cyber security responsibility Level-B.pdf
Schedule 3：Matters to be conducted by the government agency of cyber security responsibility Level-B.doc
Schedule 4：Matters to be conducted by the specific non-government agency of cyber security responsibility Level-B.pdf
Schedule 4：Matters to be conducted by the specific non-government agency of cyber security responsibility Level-B.doc
Schedule 5：Matters to be conducted by the government agency of cyber security responsibility Level-C.pdf
Schedule 5：Matters to be conducted by the government agency of cyber security responsibility Level-C.doc
Schedule 6：Matters to be conducted by the specific non-government agency of cyber security responsibility Level-C.pdf
Schedule 6：Matters to be conducted by the specific non-government agency of cyber security responsibility Level-C.doc
Schedule 7：Matters to be conducted by each agency of cyber security responsibility Level-D.pdf
Schedule 7：Matters to be conducted by each agency of cyber security responsibility Level-D.doc
Schedule 8：Matters to be conducted by each agency of cyber security responsibility Level-E.pdf
Schedule 8：Matters to be conducted by each agency of cyber security responsibility Level-E.doc
Schedule 9：Principles of classification of levels of defense requirements of information and communication system.pdf
Schedule 9：Principles of classification of levels of defense requirements of information and communication system.doc
Schedule 10：Defense standards of cyber systems.pdf
Schedule 10：Defense standards of cyber systems.doc
Article 12
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.