Cyber Security Management Act
&
Related Regulations

Executive Yuan

November 2021

Table of Contents

Part 1: The Act and Related Regulations

I. Cyber Security Management Act

1. Enacted and promulgated a total twenty-three articles of the Act by Presidential Order Hua Zong 1 Yi Zi No. 10700060021 on July 6, 2018; The implementation date of the Act shall be stipulated by the competent authority.

2. Issued by Executive Yuan Order yuan tai hu zi No. 1070217128 on December 5, 2018. The implementation date of the Act was stipulated on January 1, 2019.

Chapter 1 General Provision

Article 1 This Cyber Security Management Act (hereinafter referred to as the Act) is duly stipulated in an effort to positively carry out the national cyber security policy, accelerate the construction of environment for national cyber security to safeguard national security, and protect public interests of the entire society.

Article 2 The competent authority over the Act is the Executive Yuan.

Article 3 The terms under the Act are defined as follows:

1. Information and communication system: That refers to the system to be used to collect, control, transmit, store, circulate, delete information or to make other processing, using and sharing of such information.

2. Information and communication service: That refers to the service to be used to collect, control, transmit, store,

circulate, delete information or to make other processing, use and sharing of such information.

3. Cyber security: That refers to such effort to prevent information and communication system or information from being unauthorized access, use, control, disclosure, damage, alteration, destruction or other infringement to assure the confidentiality, integrity and availability of information and system.

4. Cyber security incident: That refers to an event where the state of the system, service or network ,through identification, likely shows violation of the cyber security policy, or failure of the security protective measures, thus adversely affect performance of information and communication system function, and constitute a threat against the cyber security policy.

5. Government agency: That refers to central, local government agency (institution) or public juristic person that exercises public power according to law, excluding military and intelligence agency.

6. Specific non-government agency: That refers to critical infrastructure provider, government-owned enterprises and government-endowed foundation.

7. Critical infrastructure: That refers to asset, system or network, either physical or virtual, once discontinued from operation or becoming less effective, would lead to

significant negative impact upon the national security, public interests, living standard of citizen and economic activities, which shall be re-examined and promulgated by the competent authority regularly.

8. Critical infrastructure provider: That refers to the ones who maintain or provide critical infrastructure either in whole or in part, as designated by the central authority in charge of relevant industry, which shall be submitted to the competent authority for ratification.

9. Government-endowed foundation: That refers to a foundation of which the operation and capital employment plan of its funds shall be submitted to the Legislative Yuan in accordance with Paragraph 3 of Article 41 of the Budget Act and its annual budget statement shall be submitted to the Legislative Yuan for deliberation in accordance with Paragraph 4 of the same Article.

Article 4 In an effort to promote cyber security, the government shall provide resources, and integrate the momentum of both civilian groups and private sectors, and boost cyber security awareness of all people, and implement the following issues:

1. Cultivation of cyber security professionals.

2. Cyber security technology research and development, integration, application, and industry-academia cooperation, as well as interchange and cooperation with international community.

3. Development of cyber security industry.

4. Development of cyber security related software and hardware specifications, relevant services and verification mechanism.

Issues Promotion in the preceding Paragraph shall be stipulated by the competent authority under the national cyber security program.

Article 5 The competent authority shall plan and promote the cyber security policy, and the cyber security technology development, and interchange and cooperation with international community, and the comprehensive cyber security protection relevant undertakings, as well as announce the report of national cyber security status, the summary auditing report on the implementation of the cyber security maintenance plan for the government agency, and the national cyber security program.

The status report, summary auditing report and the national cyber security programs of the preceding Paragraph shall be submitted to the Legislative Yuan for review.

Article 6 The competent authority may commission or entrust other government agency, juristic person or organization to implement integrated protection of cyber security, interchange and cooperation with international community, and other cyber security related issues.

The government agency, juristic person or organization, or second-tier subcontractor of the preceding Paragraph shall not divulge the secret of critical infrastructure provider which becomes known in the process of enforcement or implement of relevant issues.

Article 7 The competent authority shall stipulate the cyber security responsibility levels by considering the criteria on the importance, confidentiality and sensitivity of the business, the hierarchy of the agency, and the category, quantity and attribute of the information reserved or processed, as well as the scale and attribute of the information and communication system of the government agency and specific non-government agency. The relevant regulations regard the baseline for responsibility levels, application for a change in the level, content of obligation, staffing of dedicated personnel and other regulations and issues concerned shall be stipulated by the competent authority.

The competent authority may audit a specific non-government agency in its implementation of cyber security maintenance plan, of which the frequency, content, method and other issues concerned shall be stipulated by the competent authority.

A specific non-government agency is audited as per preceding Paragraph, and found defective or needing improvement in the cyber security maintenance program, it shall submit the improvement report to the competent

authority and tothe central authority in charge of relevant industry.

Article 8 The competent authority shall set up the cyber security information sharing mechanism.

Regulation regarding analysis, integration, and the sharing of content, procedure and method, and other matters of the cyber security information in the preceding Paragraph shall be stipulated by the competent authority.

Article 9 A government agency or specific non-government agency outsources for setup, maintenance of the cyber security system, or for provision of cyber security services, such government agency or specific non-government agency shall, within the realm of this Act, take into account outsourced party's professional capability and hands-on experience, as well as attribute of the outsourced item and requirement of cyber security, select the appropriate party for outsourcing and oversee its cyber security maintenance service.

Chapter 2 Government Agency Cyber Security Management

Article 10 A government agency shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.

Article 11 A government agency shall staff the position of Cyber Security Officer, which to be concurrently served by the deputy head or other appropriate personnel as designated by the agency head. The Cyber Security Officer shall assume the responsibility to carry out and oversee the cyber security business of the agency.

Article 12 A government agency shall submit to the superior or supervisory authority about the implementation of the cyber security maintenance plan annually. Without such superior authority, the implementation report of the cyber security maintenance program shall be submitted to the competent authority.

Article 13 A government agency shall audit the subordinate authority under its supervision about the implementation of the cyber security maintenance plan.

When an agency is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the auditing agency and the superior or the supervisory authority.

Article 14 To cope with cyber security incident, a government agency shall stipulate the reporting and responding mechanism.

When privy to a cyber security incident, the government agency shall report to the superior or supervisory authority as well as tothe competent authority. Without such superior

authority, the government agency shall report to the competent authority.

A government agency shall file a report on the investigation, handling and improvement on the cyber security incident, and shall submit the report to the superior or supervisory authority as well as the competent authority. Without a superior authority, the government agency shall submit to the competent authority.

Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority.

Article 15 Personnel with proven performance in cyber security maintenance, a government agency shall present incentive award.

Regulations for such incentive award in the preceding Paragraph shall be stipulated by the competent authority.

Chapter 3 Specific Non-Government Agency Cyber Security Management

Article 16 The central authority in charge of relevant industry shall, after consulting with the relevant government agency, civil associations, scholars and experts for their opinions, designate the critical infrastructure provider and submit to the competent authority for approval, while notifying the approved provider in writing.

A critical infrastructure provider shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.

A critical infrastructure provider shall submit to the central authority in charge of relevant industry about the implementation of the cyber security maintenance plan.

The central authority in charge of relevant industry shall audit the critical infrastructure provider about the implementation of the cyber security maintenance plan.

When a critical infrastructure provider is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the central authority in charge of relevant industry.

Regulations regarding the essentials of the cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in Paragraph 2 to Paragraph 5 shall be drafted by the central authority in charge of relevant industry, and submit to the competent authority for approval.

Article 17 A specific non-government agency other than critical infrastructure provider, shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.

The central authority in charge of relevant industry may request the specific non-government agency under their charge mentioned in the preceding Paragraph, to submit a report about implementation of the cyber security maintenance plan.

The central authority in charge of relevant industry may audit the specific non-government agency under their charge mentioned in the Paragraph 1 regarding their implementation of the cyber security maintenance plan. When found defective or needing improvement in the cyber security maintenance plan, the audited specific non-government agency shall be required to submit an improvement report before a specified date.

Regulations regarding the essentials of the cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in preceding three Paragraphs shall be drafted by the central authority in charge

of relevant industry, and submit to the competent authority for approval.

Article 18 To cope with cyber security incident, a specific non-government agency shall stipulate the reporting and responding mechanism.

When privy to a cyber security incident, a specific non-government agency shall report to the central authority in charge of relevant industry.

A specific non-government agency shall file a report on the investigation, handling and improvement on the cyber security incident and shall submit the report to the central authority in charge of relevant industry. In case of a severe cyber security incident, it shall further notify the competent authority.

Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority.

When privy to asevere cyber security incident, the competent authority or the central authority in charge of relevant industry may, in a timely manner, promulgate the essential contents of the incident and coping measures and render relevant support.

Chapter 4 Penalties

Article 19 Personnel of a government agency shall be subject to discipline or penalty in accordance with the relevant regulations if failing to comply with the regulation of the Act.

Regulations for such penalty in the preceding Paragraph shall be stipulated by the competent authority.

Article 20 If aspecific non-government agency has one among those enumerated below transpired, the central authority in charge of relevant industry shall order it to complete corrective actions within the specified time limit. If it fails to complete corrective actions within the specified time limit, it shall be subject to a fine ranging from NT$100,000 as the minimum to NT$1,000,000 as the maximum for each offense:

1. If it fails to stipulate, amend or implementthe cyber security maintenance planin accordance with Paragraph 2 of Article 16 or Paragraph 1 of Article 17, orviolates the essential items in the cyber security maintenance plan under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.

2. If it fails to submit the report on implementation of the cyber security maintenance plan to the central authority in charge of relevant industry in accordance with Paragraph 3 of Article 16 or Paragraph 2 of Article 17, or fails the requirements with the submittal of the implementation of the cyber security maintenance plan

stipulated under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.

3. If it fails the requirements under Paragraph 3 of Article 7, Paragraph 5 of Article 16 or Paragraph 3 of Article 17, unable to submit the improvement reports to the competent authority, the central authority in charge of relevant industry, or violates the regulation with the submitting of the improvement report under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.

4. If it fails to stipulate the reporting and responding mechanism of cyber security incidentin accordance with Paragraph 1 of Article 18, or violates the essential items inthe reporting and responding mechanism under Paragraph 4 of Article 18.

5. If it fails the requirements under Paragraph 3 of Article 18, unable to submit the cyber security investigation, handling and improvement reports regarding cyber security incidents to the central authority in charge of relevant industryor the competent authority, or violate the regulation with the submitting of thereport under Paragraph 4 of Article 18.

6. If it violates the regulation regarding the contents of notification under Paragraph 4 of Article 18.

Article 21 A specific non-government agency violates the provisions Paragraph 2 of Article 18, by failing to report a cyber

security incident, the central authority in charge of relevant industry shall impose a fine ranging from NT$300,000 as the minimum to NT$5,000,000 as the maximum, and shall order it to complete improvement within a specified time limit. If it fails to complete such requirement within the specified time limit, apenalty for each additional offense shall be re-imposed.

Chapter 5 Supplementary provisions

Article 22 The enforcement rules of the Act shall be stipulated by the competent authority.

Article 23 The implementation date of the Act shall be stipulated by the competent authority.

II. Enforcement Rules of Cyber Security Management Act

1. Promulgated on Novenber 21, 2018
2. Amendment promulgated on 23 August 2021

Article 1 These Rules are stipulated in accordance with Article 22 of the Cyber Security Management Act (hereinafter referred to as the Act).

Article 2 The term “military agency” as used in Subparagraph 5 of Article 3 of the Act refers to the Ministry of National Defense and its subordinate agency (institution), troop, school; and the term “intelligence agency” as used therein, refers to the agency specified in Subparagraph 1 of Paragraph 1 and Paragraph 2 of Article 3 of the National Intelligence Services Law.

Article 3 In submitting improvement reports under Paragraph 3 of Article 7, Paragraph 2 of Article 13, Paragraph 5 of Article 16 or Paragraph 3 of Article 17 of the Act, the government agency or the specific non-government agency (hereinafter referred to as “each agency”) shall submit the following contents in response to the audit result of the implementation of the cyber security maintenance plan, and shall submit the implementation of the improvement report in the manner and within the time as designated by the competent authority, superior or supervisory authority, the central authority in charge of relevant industry:

1. Flaws or items to be improved.

2. Causes of occurrence.

3. Measures in aspects of management, technology, manpower, or resource to be taken for flaws or items to be improved.

4. The estimated completion schedules of the measures under the preceding subparagraph and the tracking method on implementation progresses.

Article 4 When each agency outsources parties for setup, maintenance of information and communication system, or provision of information and communication service (hereinafter referred to as the "outsourced business") in accordance with Article 9 of the Act, attention should be paid to the following matters for the selection and supervision of the outsourced party.

1. The procedures and environment of the outsourced party in conducting outsourced business shall have completed cyber security management measures or have passed the verification of third party.

2. The outsourced party shall deploy sufficient and properly qualified and trained cyber security professionals who hold cyber security professional licenses or have similar business experience.

3. Whether the outsourced party can second-tier subcontract outsourced business' scopes and objects that may be second-tier subcontract and the cyber

security maintenance measures that the second-tier subcontractor should have.

4. If the outsourced business involves classified national security information, the person who conduct the outsourced business shall be reviewed and the departure shall be controlled in accordance with the Classified National Security Information Protection Act.

5. If the outsourced business includes customized development of information and communication system, the outsourced party shall provide security testing certificate of such information and communication system; if such information and communications system is the core system of the outsourcing agency, or the outsourcing amount exceeds NT$10,000,000, the outsourcing agency shall conduct itself or contract third party to conduct the security testing; if the use of system or resource other than those developed by the outsourced party is involved, content and source of those not developed by the outsourced party shall be indicated and the certification of authorization thereof shall be provided.

6. If the outsourced party conducts outsourced businesses in violation of the relevant regulatory requirement of cyber security or becomes aware of cyber security incident, it shall immediately notify the outsourcing agency thereof and take remedy measure therefor.

7. If the entrusting relationship is terminated or canceled, it shall be confirmed that the outsourced party has returned, handed over, deleted or destroyed all materials in its possession for the performance of the contract.
8. The outsourced party shall take other relevant measure for cyber security.
9. The outsourcing agency shall, periodically, or whenever it becomes aware of the occurrence of cyber security incident of the outsourced party that might affect the outsourced business, confirm the implementation status of the outsourced business by audit or other appropriate method.

In conducting the competency audit under Subparagraph 4 of the preceding paragraph, the outsourcing agency shall take into consideration the confidential level and content of the classified national security information in which the outsourced business is involved, and shall, to the necessary extent, check whether the personnel of the outsourced party who performs such business or other personnel who might access such classified national security information has any of the following circumstances:

1. One who had committed the offense of disclosing secret, or had committed the offense of civil disturbance or treason after the termination of the Period of National Mobilization in Suppression of Communist Rebellion, and was finally convicted, or was put on a wanted list

which has not been closed.

2. One who was aformer public official, was subject to administrative penalty or demerit record due to a violation of relevant regulatory for security confidentiality.

3. One who was induced or coerced by foreign government, mainland China, Hong Kong or Macau government to engage in activity unfavorable to national security or significant interest of the nation.

4. Other concrete item relating to the protection of classified national security information.

The circumstance under Subparagraph 4 of Paragraph 1 shall be stated in the tender notice, tender document and contract; before the verification of the competency audit, the relevant personnel shall agree in writing document.

Article 5 The "inwriting" document under Paragraph 3 of the preceding article and Paragraph 1 of Article 16 of the Act may be the electronic one in accordance with the Electronic Signatures Act.

Article 6 The cyber security maintenance plan under Article 10, Paragraph 2 of Article 16, and Paragraph 1 of Article 17 of the Act shall include the following:

1. Core businesses and their significance.

2. Cyber security policy and objectives.

3. The organization promoting cyber security.
4. The deployment of dedicated manpower and fund.
5. The deployment of Cyber Security Officer of the government agency.
6. The inventory of information and communication systems and information, and indicating the core ones and relevant assets.
7. Risk assessments of cyber security.
8. Protection and control measures for cyber security.
9. The notification, response and rehearsal mechanisms relating to cyber security incidents.
10. Cyber security information assessment and response mechanism.
11. Management measures for outsourced information and communication system or service.
12. Assessment mechanism for personnel of the government agency who conducts business involving cyber security matters.
13. The continual improvement and performance management mechanism for the cyber security maintenance plan and implementation status.

The implementation of cyber security maintenance plans submitted by each agency under Article 12, Paragraph 3 of

Article 16, or Paragraph 2 of Article 17 of the Act shall include the implementation results of and relevant explanations for those under each subparagraph of the preceding paragraph.

The stipulation, amendment, and implementation of the cyber security maintenance plans under Paragraph 1, and the submission of the implementation thereof to be conducted by a government agency may, with consent of its superior or supervisory authority, be conducted by its superior or supervisory authority or another government agency subordinate to its superior or supervisory authority; and in case of a specific non-government agency, the same may, with consent of its central authority in charge of relevant industry, be conducted by its central authority in charge of relevant industry, a subordinate government agency of such central authority in charge of relevant industry, or another specific non-government agency regulated by the central authority in charge of relevant industry.

Article 7 The scope of the core businesses specified in Subparagraph 1 of Paragraph 1 of the preceding article are as follows:

1. Businesses that are considered as the core accountabilities of the government agency as determined by its organizational regulation.
2. Major services or functions of government-owned enterprise and government-endowed foundation.

3. Businesses that are required by each agency for the maintenance and provision of critical infrastructure.

4. Businesses in which each agency is involved in accordance with Paragraphs 1 to 5 of Article 4, or Paragraphs 1 to 4 of Article 5 of the Regulations on Classification of Cyber Security Responsibility Levels.

The term "core information and communication system" as used in Subparagraph 6 of Paragraph 1 of the preceding article refers to the system that is necessary for supporting the continual operation of core business, or that is of high level of defense requirements as determined in accordance with Schedule 9 to the Regulations on Classification of Cyber Security Responsibility Levels – principles of classification of cyber system defense requirement levels.

Article 8 The investigation, handling and improvement report on cyber security incident under Paragraph 3 of Article 14 and Paragraph 3 of Article 18 of the Act shall include the following:

1. Times of the occurrences of or the awareness of the occurrences of the incidents, the completion of damage control or recovery operations.

2. The scope affected by the incidents and the damage assessment.

3. The courses of damage control and recovery operations.

4. The courses of incident investigations and handling

operations.

5. Cause analysis of the incident.

6. Measures in aspects of management, technology, manpower or resources taken to prevent the reoccurrences of similar incident.

7. The estimated completion schedule and the follow-up mechanism of the measures under the preceding subparagraph.

Article 9 Before designating critical infrastructure providers under Paragraph 1 of Article 16 of the Act, the central authority in charge of relevant industry shall give such providers the opportunity to state their opinions.

Article 10 The term “severe cyber security incident” as used in Paragraphs 3 and 5 of Article 18 of the Act refer to level-3 and level-4 cyber security incidents specified in Paragraphs 4 and 5 of Article 2 of the Regulations on the Notification and Response of Cyber Security Incidents.

Article 11 When the competent authority or the central authority in charge of relevant industry is privy to a cyber security incident and publicize the necessary contents and countermeasures relating to severe cyber security incidents under Paragraph 5 of Article 18 of the Act, upon awareness of such incidents, times of occurrence or privy of the occurrence, causes, affection degree, control status, and subsequent improvement measures of such incidents shall

be stated in the publications.

Under any of the following circumstances, the necessary contents and contingency measures relating to the incidents under the preceding paragraph shall not be publicized:

1. If it involves trade secrets or information relating to business operations of individuals, juristic persons or organizations or if the disclosure might infringe upon rights or other rightful interests of the government agency, individual, juristic person or organizations; except as is otherwise required by law, or necessary for public welfare or necessary for protection of life, body, and health of people, or with consent of the parties concerned.
2. Other circumstances of confidentiality, restriction, or prohibition on disclosure as required by law.

If the necessary contents and contingency measure relating to the incidents shall not be publicized under Paragraph 1, only the other portion may be publicized.

Article 12 If businesses of the specific non-government agency involve the accountabilities of several central authority in charge of relevant industry, the competent authority may designate via coordination more than one central authority in charge of relevant industry to solely or jointly conduct the matters to be conducted by the central authority in charge of relevant industry under the Act.

Article 13 The implementation date of the Rules shall be stipulated by the competent authority.

The amendments to these Enforcement Rules shall take effect on the date of promulgation.

III. Regulations on Classification of Cyber Security Responsibility Levels

1. Promulgated on Novenber 21, 2018
2. Amendment promulgated on 26 August 2019
3. Amendment promulgated on 23 August 2021

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.

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.

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

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the government agency shall inspect the appropriateness of the classification of levels of the information and communication systems at least once a year.
	The importation of the information security management system and verification by a impartial third party		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of levels, the government agency shall deploy four persons on a full-time basis.
	Internal cyber security audits		Conduct twice a year.
	Business sustainable operation rehearsals		Conduct once a year for all core information and communication systems.
	Cyber governance maturity assessment		Conduct once a year.
	Restricted use of threatening national cyber security products		1. Except for business needs and no other alternatives, it is not allowed to purchase and use the threatening national cyber security products that are produced, researched, developed, manufactured or provided by the manufacturers approved by the competent authority.

			2. When purchasing or using a threatening national cyber security product, it shall specify the reasons and purchase it on a case-by-case basis after receiving approval from the competent authority. 3. For the threatening national cyber security products that was used before the amendment to the Regulation took effect or that was approved by the competent authority for business needs and have no other alternatives, they should be listed for management and should not be interfaced with the official network environment.
Technical aspect	Security detection	Vulnerability scanning	Conduct twice a year for all core information and communication systems.
		Penetration test	Conduct once a year for all core information and communication systems.
	Cyber security health diagnosis	Inspection of network frameworks	Conduct once a year.
		Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Cyber security threat detection management mechanisms		Within one year after receipt of initial approval or change of level, the government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof and submit the monitoring management documentation in the manner designated by the competent authority. The monitoring scope shall include the

		contents conducted for “Endpoint detection and response mechanism” and “Cyber security defense” as specified in this Schedule, the cyber equipment records of the active directory system and the agency’s core information and communication system, and the records of information service or the application.
	Government configuration baseline	Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of government configuration standards for the items publicized by the competent authority and shall continue the maintenance and operation thereof.
	Vulnerability alert and notification system mechanism	1. Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of the vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the government agency shall, within one year of the enforcement of the amendments, complete the import operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Endpoint detection and response mechanism	1. Within two years of receipt of initial approval or change of levels, the government agency shall complete the import operation of endpoint detection and response mechanism, and shall continue the maintenance and operation thereof and submit the detection data in the manner designated by the competent authority.

			2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the government agency shall, within two years of the enforcement of the amendments, complete the endpoint detection and response mechanism, continue the maintenance and operation thereof and submit the detection data in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewalls	
		If the government agency has email servers, it should have email filtering mechanisms	
		Intrusion detection and defense mechanism	
		If the government agency has core information and communication systems for external services, it should have the application firewalls	
		Defense measures for advanced persistent threat attacks	
Awareness and training	Cyber security education and training	Full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.

		General user and officer	Each year, each person shall receive general cyber security education training for not less than three hours.
	Cyber security professional license and competence training certificates		1. Within one year after receipt of initial approval or change of levels, at least four full-time cyber security persons shall each hold one or more licenses and certificates, and shall continually maintain the validity of the licenses and certificates. 2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in "impartial third-party certification" refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certificate issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.
4. In conducting "cyber security health diagnosis" of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.
5. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
6. Endpoint detection and response mechanism refers to the protective operations with functions of active scanning and detecting on endpoint, vulnerability protection, analysis of suspicious program or abnormal activities and display function of the level of relevant threats.
7. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.

Schedule 2: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-A

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of the information and communication systems at least once a year.
	The importation of the information security management system and verification by a impartial third party		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the specific non-government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of levels, the specific non-government agency shall deploy four persons.
	Internal cyber security audits		Conduct twice a year
	Business sustainable operation rehearsal		Conduct once a year for all core information and communication systems
Technical aspect	Security detection	Vulnerability scanning	Conduct twice a year for all core information and communication systems

		Penetration test	Conduct once a year for all core information and communication systems
	Cyber security health diagnosis	Inspection of network frameworks	Conduct once a year
		Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connection	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof. The monitoring scope shall include the contents conducted for "Cyber security defense" as specified in this Schedule, the cyber equipment records of the active directory system and the agency's core information and communication system, and the records of information service or the application.
	Vulnerability alert and notification system mechanism		1. Within one year after receipt of initial approval or change of level, the critical infrastructure provider shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the

			manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the critical infrastructure provider shall, within one year of the enforcement of the amendments, complete the import operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewalls	
		If the specific non-government agency has email servers, it should have email filtering mechanisms	
		Intrusion detection and defense mechanism	
		If the specific non-government agency has core information and communication systems for external services, it should have the application firewalls	
		Defense measures for advanced persistent threat attacks	

Awareness and training	Cyber security education and training	Dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours
	Cyber security professional licenses		1. Within one year after receipt of initial approval or change of levels, at least four dedicated cyber security persons shall each hold one or more licenses, and shall continually maintain the validity of licenses. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in "impartial third-party certification" refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certificate issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. In conducting "cyber security health diagnosis" of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by the central authority in charge of relevant industry.
4. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.

5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.
6. The central authority in charge of relevant industry of the specific non-government agency may, depending on the actual requirements and to the extent of compliance with these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

Schedule 3: Matters to be conducted by the government agency of cyber security responsibility Level-B

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year.
	The importation of the information security management system and verification by a impartial third party		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of levels, the government agency shall deploy two persons on full-time basis.
	Internal cyber security audits		Conduct once a year.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
	Cyber governance maturity assessment		Conduct once a year.
Technical aspect	Security detection	Vulnerability scanning	Conduct once a year for all core information and communication systems.

		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber security health diagnosis	Inspection of network frameworks	Conduct once every two years.
		Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Cyber security threat detection management mechanisms		Within one year after receipt of initial approval or change of level, the government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof and submit the monitoring management documentation in the manner designated by the competent authority. The monitoring scope shall include the contents conducted for "Endpoint detection and response mechanism" and "Cyber security defense" as specified in this Schedule, the cyber equipment records of the active directory system and the agency's core information and communication system, and the records of information service or the application.
	Government configuration baseline		Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of government configuration baseline for the items publicized by the competent authority,

		and shall continue the maintenance and operation thereof.
	Vulnerability alert and notification system mechanism	1. Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of the vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the government agency shall, within one year of the enforcement of the amendments, complete the import operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Endpoint detection and response mechanism	1. Within two years of receipt of initial approval or change of levels, the government agency shall complete the import operation of Endpoint detection and response mechanism, and shall continue the maintenance and operation thereof and submit the detection data in the manner designated by the competent authority. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, the government agency shall, within two years of the enforcement of the amendments, complete the Endpoint detection and response mechanism, and shall continue the maintenance and operation thereof and submit the detection data in the manner

			designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewalls	
		If the government agency has email servers, it should have email filtering mechanisms	
		Intrusion detection and defense mechanism	
		If the government agency has core information and communication systems for external services, it should have the application firewalls	
Awareness and training	Cyber security education and training	Full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours

	Cyber security professional license and competence training certificates	1. Within one year after receipt of initial approval or change of levels, at least two full-time cyber security persons shall each hold one or more license(s) and certificate(s), and shall continually maintain those validity. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in "impartial third-party certification" refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certification issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.
4. In conducting "cyber security health diagnosis" of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.
5. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
6. Endpoint detection and response mechanism refers to the protective operations with functions of active scanning and detecting on endpoint, vulnerability protection, analysis of suspicious program or abnormal activities and display function of the level of relevant threats.
7. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.

Schedule 4: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-B

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year.
	The importation of the information security management system and verification by a impartial third party		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the specific non-government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of levels, the specific non-government agency shall deploy two persons.
	Internal cyber security audits		Conduct once a year.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
Technical aspect	Security detection	Vulnerability scanning	Conduct once a year for all core information and communication systems.
		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber security	Inspection of network frameworks	Conduct once every two years.

	health diagnosis	Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of levels, the specific non-government agency shall complete the development of threat detection mechanisms, and shall continue the maintenance and operation thereof. The monitoring scope shall include the contents conducted for "Cyber security defense" as specified in this Schedule, the cyber equipment records of the active directory system and the agency's core information and communication system, and the records of information service or the application.
	Vulnerability alert and notification system mechanism		1. Within one year after receipt of initial approval or change of level, the critical infrastructure provider shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the critical infrastructure provider shall, within one year of the enforcement of the amendments, complete the import operation of

			the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewalls	
		If the specific non-government agency has email servers, it should have email filtering mechanisms	
		Intrusion detection and defense mechanism	
		If the specific non-government agency has core information and communication systems for external services, it should have the application firewalls	
Awareness and training	Cyber security education and training	Dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional licenses		1. Within one year after receipt of initial approval or change of levels, at least two dedicated cyber security

		persons shall each hold one or more license(s) and certificate(s), and shall continually maintain those validity. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in "impartial third-party certification" refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certificate issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. In conducting "cyber security health diagnosis" of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by the central authority in charge of relevant industry.
4. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.
6. The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

Schedule 5: Matters to be conducted by the government agency of cyber security responsibility Level-C

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9; subsequently, the government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year. If the system levels are "high", the government agency shall, within two years of receipt of initial approval or change of levels, complete the control measures specified in Schedule 10.
	The importation of the information security management system		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority, and shall continually maintain the importation thereof.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of levels, the government agency shall deploy one person on a full-time basis.
	Internal cyber security audits		Conduct once every two years.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
Technical aspect	Security detection	Vulnerability scanning	Conduct once every two years for all core information and communication systems.
		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber security health diagnosis	Inspection of network frameworks	Conduct once every two years.
		Inspection of malicious cyber activities	

		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Vulnerability alert and notification system mechanism		1. Within two years after receipt of initial approval or change of level, the government agency shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations on August 23, 2021, the government agency shall, within two years of the enforcement of the amendments, complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewalls	
		If the government agency has email servers, it should have	

		email filtering mechanisms	
Awareness and training	Cyber security education and training	Full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional license and competence training certificates		Within one year after receipt of initial approval or change of levels, at least one full-time cyber security personnel shall hold one or more license(s) and certificate(s), and shall continually maintain the validity of the licenses and certificates.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.
3. In conducting "cyber security health diagnosis" of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.
4. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.

Schedule 6: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-C

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classifications of levels of the information and communication systems developed by itself or outsourced according to Schedule 9; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year. If the system levels are "high", the specific non-government agency shall, within two years of receipt of initial approval or change of levels, complete the control measures specified in Schedule 10.
	The importation of the information security management system		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority, and shall continually maintain the importation thereof.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of levels, the specific non-government agency shall deploy one person.
	Internal cyber security audits		Conduct once every two years.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
Technical aspect	Security detection	Vulnerability scanning	Conduct once every two years for all core information and communication systems.
		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber security	Inspection of network frameworks	Conduct once every two years.

	health diagnosis	Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Vulnerability alert and notification system mechanism		1. Within two years after receipt of initial approval or change of level, the critical infrastructure provider shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations on August 23, 2021, the critical infrastructure provider shall, within two years of the enforcement of the amendments, complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the
		Network firewalls	
		If the specific non-government	

		agency has email servers, it should have email filtering mechanisms	necessary update or upgrading of software and hardware.
Awareness and training	Cyber security education and training	Dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional licenses		Within one year after receipt of initial approval or change of levels, at least one dedicated cyber security personnel shall hold one license or more, and shall continually maintain the validity.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. In conducting "cyber security health diagnosis" of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by central authority in charge of relevant industry.
3. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
4. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.
5. The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

Schedule 7: Matters to be conducted by each agency of cyber security responsibility Level-D

System aspect	Items conducted	Sub-items conducted	Contents conducted
Technical aspect	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, each agency shall complete activation of various cyber security defense measures and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewalls	
		If each agency has email servers, it should have email filtering mechanisms	
Awareness and training	Cyber security education and training	General users and officers	Each year, each person shall receive general cyber security education training for not less than three hours.

Note: The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

Schedule 8: Matters to be conducted by each agency of cyber security responsibility Level-E

System aspect	Items conducted	Sub-items conducted	Contents conducted
Awareness and training	Cyber security education and training	General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.

Note: The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

Schedule 9: Principles of classification of levels of defense requirements of information and communication system

Defense requirements Levels Dimension	High	Medium	Common
Confidentiality	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to limited impact on the operation, asset or reputation of the agency.
Integrity	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to limit impact on the operation, asset or reputation of the agency.
Availability	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to limit impact on the operation, asset or reputation of the agency.

Regulatory compliance	The failure to strictly comply with regulatory requirements relating to the establishment or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the personnel of the agencies to be subject to criminal liabilities.	The failure to strictly comply with regulatory requirements relating to the establishment or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the agencies or their personnel to be subject to administrative punishments, disciplines or penalties.	Other status of establishment or operation of information and communication system under relevant regulatory requirements.

Note: The defense requirement levels of the information and communication system shall be the highest ones as determined in any of the dimensions of confidentiality, integrity, availability and regulatory compliance relating to such systems.

Schedule 10: Defense standards of cyber systems

Defense requirements of systems Levels Control measures		High	Medium	Common
Dimension	Contents of the measures			
Access control	Account management	1. The agency shall define the idle time or usable duration of each system and the use status and condition of information and communication system. 2. When the permitted idle time prescribed by the agency or usable time is exceeded, the system should automatically logout the users. 3. Use the information and communication system according to the circumstances and conditions prescribed by the agency. 4. Monitor the information and communication system accounts; report to the administrator if any abnormal use by an account is found 5. All control measures for the level of "medium".	1. The temporary or emergent accounts which have expired should be deleted or prohibited. 2. The idle accounts of information and communication system should be prohibited. 3. Periodically review the application, establishment, revision, activation, suspension and deletion of accounts of information and communication systems. 4. All control measures for the level of "common".	Establish the account management mechanism, including the procedure for application, establishment, revision, activation, suspension and deletion.
	Least privilege	The principle of least privilege is adopted. The users(or the procures for acts on behalf of users)are granted authorized access required for the completion of duties only, depending on the duties and business functions of the agencies .		No requirement

	Remote access	1. Any remote connection with the cyber system should be monitored. 2. The cyber system should adopt encryption mechanisms. 3. The source of remote access to the cyber system should be the access control point as pre-defined and managed by the agencies. 4. All control measures for the level of "common".	1. For each kind of permitted remote access, the authorization should be obtained in advance; the use restriction, configuration requirement, connection requirement and documentation should be established. 2. The inspection operation of users' privilege should be completed at the server terminal. 3. The remote access to intranet of the agency or the connection to the information and communication system back office should be monitored. 4. Encryption mechanism should be adopted.
Event log and accountability	Record events	1. The log generated by the information and communication system which is retained by the agency should be reviewed periodically. 2. All control measures for the level of "common".	1. Stipulate the time cycle of records in the logs and retention policy and retain the logs for at least six months. 2. Assure that the information and communication system has the function of record of specific events, and determine the specific information and communication system incidents to be recorded. 3. Should record various functions executed by the administrator

				account of the information and communication system.
	Content of log record	The log generated by the information and communication system shall include the type of incidents, dates of occurrence, places of occurrence, and the information about the identification of the users relating to the incidents; the single log mechanism should be adopted to assure the consistency of the formats of output, and other relevant information shall be included in accordance with the cyber security policy and requirements of laws and regulations.		
	Storage capacity of the log	Storage capacity required for the log shall be equipped depending on the requirement of the storage of the log.		
	Response to failure in log process	1. Upon occurrence of the event of failure in log process which should be reported immediately as required by the agency, the information and communication system should give warnings to the specific personnel within the timeframes prescribed by the agency. 2. All control measures for the levels of "medium" and "common".		In case of failure in log process, the information and communication system should take appropriate actions.
	Time stamp and time calibration	1. The internal clock of the system should periodically synchronize with the time cycle specified by the agency and the source of standard times. 2. All control measures for the level of "common".		The information and communication system should use the internal clock of the system to generate time stamps required for the log, and such time stamps should be able to correspond to Universal Time Coordinated(UTC) or Greenwich Mean Time(GMT).
	Protection of log information	1. Periodically back up the log to the physical system different from the original audit system. 2. All control measures for the level of "medium"	1. Should use the integrity of the hashing or other proper methods to assure the mechanism. 2. All control measures for the level of "common".	The access management of the log is limited to the users with privileges.
Business continuity plan	Backup of system	1. Should take the backup and restore as a part of the testing of the business continuity plan. 2. Should store the important software of the information and communication	1. Should periodically test the backup information to verify the reliability of the backup media and the integrity of the information. 2. All control measures for the level of "common".	1. Set the requirement for tolerable time of information loss of the system. 2. Execute the system source codes and the data backup.

		system and backup of other security related information in the independent facilities or fire cabinets at the place different from the operating systems. 3. All control measures for the level of "medium".		
	System rescue	1. Set the requirements for the tolerable time from the interruption of information and communication system to the recovery of service. 2. When the original service interrupts, the service is provided by the rescue equipment or other method in lieu thereof within the tolerable time.		No requirement
Audits and accountabilities	Audit events	1. Audit events should be reviewed periodically. 2. All control measures for the level of "common".		1. Retain audit records according to the prescribed time cycle and the policies of record retention. Assure that the cyber system has the function of audit of specific events, and determine the specific cyber system incidents to be audited. 2. Should audit various functions executed by the administrator account of the cyber system.
	Contents of audit records	1. Audit records generated by the cyber systems shall include other relevant information as required. 2. All control measures for the level of "common".		Audit records generated by the cyber system shall include the type of incidents, date of occurrence, place of occurrence, and information about the identification of the users relating to the

				incidents; single journal recording mechanisms should be adopted to assure the consistency of the formats of output.
	Storage capacity for the audits	Storage capacity required for the audit records shall be equipped depending on the requirement of the storage of audit records.		
	Response to failure in audit process	1. Upon occurrence of audit failure events, which should be reported immediately as required by the agencies, the cyber systems should give warnings to the specific personnel within the timeframes prescribed by the agencies. 2. All control measures for the levels of "medium" and "common".		In case of failure in the audit process, the cyber systems should take appropriate actions.
	Time stamp and time calibration	1. The internal clock of the system should synchronize with the time cycle specified by the agencies and the source of standard times. 2. All control measures for the level of "common".		The cyber systems should use the internal clock of the systems to generate time stamps required for audit records, and such time stamps should be able to correspond to Universal Time Coordinated(UTC) or Greenwich Mean Time(GMT).
	Protection of log information	1. Periodically back up the log to the physical system different from the original audit system. 2. All control measures for the level of "medium"	1. Should use the integrity of the hashing or other proper methods to assure the mechanism. 2. All control measures for the level of "common".	The access management of the log is limited to the users with privileges.
Business continuity plan	Backup of system	1. Should take the backup and restore as a part of the testing of the business continuity plan. 2. Should store the important software of the	1. Should periodically test the backup information to verify the reliability of the backup media and the integrity of the information.	1. Set the requirement for tolerable time of information loss of the system. 2. Execute the system source codes and the data backup.

		information and communication system and backup of other security related information in the independent facilities or fire cabinets at the place different from the operating systems. 3. All control measures for the level of "medium".	2. All control measures for the level of "common".	
	System rescue	1. Set the requirements for the tolerable time from the interruption of information and communication system to the recovery of service. 2. When the original service interrupts, the service is provided by the rescue equipment or other method in lieu thereof within the tolerable time.		No requirement
Identification and authentication	Identification and authentication of internal users	1. Adopt multiple authentication technologies for the access to the information and communication system. 2. All control measures for the level of "medium" and "common".		The information and communication system should have the function of identification and authentication of sole agency users(or the program of act on behalf of agency users); common accounts are prohibited.
	Identity verification management	1. Identity verification mechanism should prevent from the logon by automatic program or the trials of change of password. 2. The password resetting mechanisms have verified identities of users again, and then send one-time and time-based tokens. 3. All control measures for the level of "common".		1. When using the preset password to login the system, should immediately change the password after logon. 2. Information relating to identity verification may not be transmitted by plain text. 3. Have the account lockout mechanism; if the identity verification for account logon fails for five times, disallow such account to continue the trial of logon at least within fifteen minutes, or use the failure verification

			mechanisms built by the agencies themselves. 4. While the password is used to conduct authentication, the least complexity of password should be imposed; and the restriction on the shortest and longest validity of passwords should be imposed. 5. In the event of change of password, at least the password may not be same as those used for previous three times. 6. The measures specified in points 4 and 5 may be conducted for non-internal users according to the regulations formulated by the agencies themselves.
	Authentication information feedback	The information and communication system should shield the information in the course of authentication.	
	Encryption module authentication	When the information and communication systems use the passwords for authentication, such passwords should be encrypted, or stored after hashing process.	No requirement
	Identification or authentication of non-internal users	The information and communication systems should identity and authenticate non-internal users (or the program of act on behalf of agency users).	
Access to systems and services	Requirement phase of system development life circle	Use the method of checklist to confirm system security requirements(including confidentiality, availability and integrity).	
	Design phase of system development life circle	1. Depending on the system functions and requirements, identify the threats that might impact on the system, to conduct risk analysis and assessment. 2. Feedback the risk assessment results to the screening items of the requirement phase and submit the revision of security requirements.	No requirement
	Development phase of system development life circle	1. Execute "source code scanning" security testing. 2. The system should have the notification mechanisms when serious error occurs.	1. Should practice necessary control measures for the security requirements.

		3. All control measures for the level of "medium" and "common".		2. Should pay attention to the avoidance of common software vulnerabilities, and practice necessary measures. 3. When errors occur, the user's pages display short error message and code only, without detailed error message.
	Testing phase of system development life circle	10. Execute "penetration testing" security testing. 11. All control measures for the level of "medium" and "common".		Execute "vulnerability scanning" security testing.
	Deployment and maintenance operation phase of system development life circle	1. In the maintenance operation phase of system development life circle, the version control and change management shall be implemented. 2. All control measures for the level of "common".		1. Under the deployment environment, should conduct update and fixing of relevant cyber security threats, and close unnecessary services and ports. 2. Not to use preset passwords for information and communication system.
	Outsourcing phase of system development life circle	If the development of the information and communication system is outsourced, the security requirements by level (including confidentiality, availability, integrity) for each phase of system development life circle shall be included in the outsourcing contract.		
	Obtaining programs	Development, testing, and formal operation environments should be separated.		No requirement
	System documents	Should store the documents relating to the management system development life circle.		
Protection of systems and communications	confidentiality and integrity of transmission	1. The information and communication system should adopt encryption mechanism, to prevent from unauthorized disclosure of information or to detect the change of information; unless there are substitutive physical protection measures in the course of transmission.	No requirement	No requirement

		2. Use public, international institution verified and not cracked algorithms. 3. Support the maximum length key of algorithms. 4. Periodically change the encryption key or certification. 5. Should formulate the management regulations on the custody of key at server terminal, and implement security defense measures that should exist.		
	Securities of data storage	The important configuration setting file of the information and communication system and other relevant confidential information required for protection should be encrypted or stored by other appropriate method.	No requirement.	No requirement.
Integrity of systems and information	Vulnerability fixing	1. Periodically confirm the status of fixing of relevant vulnerabilities of the information and communication system. 2. All control measures for the level of "common".		The vulnerability fixing of the system should be tested for the effectiveness and potential impact, and should be updated periodically.
	Monitoring of information and communication system	1. The information and communication system should adopt automatic tools to monitor the access communication flows; if unusual or unauthorized activities are found, conduct the analysis of such activity. 2. All control measures for the level of "medium".	1. Monitor the information and communication system to detect the attack and unauthorized connection and to identify the unauthorized users of the information and communication system. 2. All control measures for the level of "common".	If a sign of hacking to the information and communication system is found, should notify the specific personnel of the agencies thereof.
	The integrity of software and information	1. Should conduct the inspection of the integrity of software and information. 2. All control measures for the level of "medium".	1. Use the integrity verification tools to detect the unauthorized change of specific software and information. 2. The examination of the legitimacy of input data of users should be placed on	No requirement

			the server terminal of the application system. 3. If any violation to the integrity is found, the information and communication system should implement the security defense measures designated by the agency.	

Notes: The central authority in charge of relevant industry of the specific non-government agency may, depending on the actual requirements and to the extent of compliance with these Regulations, otherwise provide for the information and communication system defense standards of its regulated specific non-government agency.

IV. Regulations on the Notification and Response of Cyber Security Incident

1. Promulgated on Novenber 21, 2018

2. Amendment promulgated on 23 August 2021

Chapter 1 General Provisions

Article 1 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").

Article 2 Cyber security incident is classified into four levels.

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:

1. Minor breach of non-core business information.
2. Minor alteration of non-core business information or non-core information and communication system.
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.

The cyber security incident occurred to each agency under any of the following circumstances is the level-2 cyber security incident:

1. Serious breach of non-core business information or minor breach of core business information not involving the maintenance and operation of critical infrastructures.
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.
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.

The cyber security incident occurred to each agency under any of the following circumstances is the level-3 cyber security incident:

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.

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.

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.

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:

Within seventy-two hours of the awareness of a level-1 or level-2 cyber security incident;

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.

V. Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency

1. Promulgated on Novenber 21, 2018

2. Amendment promulgated on 23 August 2021

Article 1 These Regulations are stipulated in accordance with Paragraph 2 of Article 7 of the Cyber Security Management Act.

Article 2 These Regulations stipulate “in writing” document may be an electronic document in accordance with the provisions of the Electronic Signatures Act.

Article 3 Except for cause by force majeure, the competent authority shall select and determine the specific non-government agencies (hereinafter referred to as the “audited agency”) for each quarter of the year, and may audit the implementation of their cyber security maintenance plans through onsite audit every year.

In selecting and determining the audited agencies under the preceding paragraph, the competent authority shall give comprehensive consideration to the significance and confidential sensitivities of its businesses, the size and nature of their cyber systems, the frequencies and degrees of occurrence of cyber security incidents, the results of cyber offense and defense exercise, the frequencies and results of audits conducted by the competent authority or

the central authority in charge of the relevant industry over past years, or other factors relating to cyber security.

In conducting the audit under Paragraph 1, the competent authority shall establish the audit program, the content of which shall include the basis and purposes, time period, essential fields of the audit, the manner of formation of the audit team, confidentiality obligation, the method, standards and items of the audit, and assistance issues from the central authority in charge of relevant industry.

In determining the essential fields, standards and items of the audit under the preceding paragraph, the competent authority shall take into comprehensive consideration the cyber security policy of our country, domestic and foreign cyber security trends, the contents and results of past audit programs, and any other factors relating to the proper allocation of audit resources or audit effectiveness.

Article 4 In conducting the audit under Paragraph 1of the preceding article, the competent authority shall deliver the audit program notice in writing to the audited agency one month before the audit.

Due to business factor or other justifiable reason, the audited agency may apply to the competent authority for adjustment of the audit date within five days of the receipt of the preceding notice in writing.

The preceding application is limited to one time except for the case of force majeure.

Article 5 In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the audited agency to give explanations on, to collaborate the implementation of cyber security maintenance plan, or provide relevant documents and supporting information for onsite inspection, and conduct the following issues. The audited agency and its personnel shall cooperate accordingly:

1. Pre-audit interview.

2. Onsite physical audit.

The audited agency cannot give the explanations, collaborate or provide documentation for onsite inspector under the preceding paragraph for justifiable reasons under the law, they shall submit the reasons in writing to the competent authority.

Upon receipt the preceding notice in writing, the competent authority shall verify it and then take the following actions, and may suspend all or part of the audit operations:

1. If the reasons are considered justifiable, it shall record the accordance and relevant information in the audit report.

2. If the reasons are considered groundless, it shall require the audited agency to follow the requirements of Paragraph 1; if the audit operations have been suspended, it may select other time periods to continue

the audit and deliver the audit program notice in writing to the audited agency ten days before the audit.

Article 6 In conducting the audit under Paragraph 1 of Article 3, the competent authority shall form an audit team composed of three to more people respectively for each audited agency, depending on the considerations under Paragraph 2 of the same article.

Informing the audit team under the preceding paragraph, the competent authority shall, taking the needs of the audit into consideration, invite representatives of government agencies or experts and scholars who have professional knowledge of cyber security policies or have professional knowledge of technologies, managements, law affairs required for such audit to act as members of such team, of which the number of representatives of the government agency may not be less than one-fourth of all members.

The competent authority shall sign, in writing, with members of audit teams on recusal due to interest conflicts and confidentiality obligations.

If the member of audit team under Paragraph 2 has any of the following circumstances, he shall avoid himself from acting as the member of that audit team:

1. He, his spouse, his relatives within the third degree, his family member, or the trustee of the property trusts of above-mentioned persons have a property or non-

property interest relationship with the audited agency or the responsible person thereof.

2. He, his spouse, his relatives within the third degree or his family member has employment, contract, appointment, agency or other similar relationship with the audited agency or the responsible person in the current or the past two years.

3. He has served in the current or past two years to be a consultant of the audited agency and his mentoring project is related to the audit program.

4. Other circumstance that may be considered that his role as a member of the audit team might affect the impartiality of the audit result.

Article 7 The competent authority shall, within one month after the completion of the audit operations on the audited agency as designated for each quarter, deliver the audit reports to the audited agencies for the quarter.

The contents of the preceding audit reports shall include the scope of the audit, flaws or items to be improved, the status and reasons for the failures of the audited agency to give explanations, collaborate or provide documentations for on-site inspections under Paragraph 2 of Article 5, and the audit results of the competent authority under Paragraph 3 of the same article, and other necessary contents relating to the audit.

Article 8 If flaws or items to be improved are found in the implementation of the cyber security maintenance plan, the audited agency shall submit improvement report in the manner specified by the competent authority within one month after the competent authority has delivered the audit report, and shall deliver the same to the central authority in charge of the relevant industry. The competent authority and the central government authority in charge of the subject industry may require the audited agency to give explanations or make adjustments when necessary.

After the improvement reports are submitted under the preceding paragraph, the audited agency shall submit the implementation status of the improvement reports in the manner and within the timeframe specified by the competent authority, and shall deliver the same to the central authority in charge of the relevant industry. The competent authority may require the audited agency to give explanations or make adjustments when necessary.

Article 9 In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the central authority in charge of the relevant industry with the audited agency to dispatch personnel for necessary assistance.

Article 10 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.

VI. Cyber Security Information Sharing Regulations

Promulgated on Novenber 21, 2018

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.

Part 2: The comparison table of Chinese and English

資通安全管理法-英譯對照

資通安全管理法	Cyber Security Management Act
第一章　　總則	Chapter I. General Provision
第一條　為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。	Article 1. This Cyber Security Management Act (hereinafter referred to as the Act) is duly stipulated in an effort to positively carry out the national cyber security policy, accelerate the construction of environment for national cyber security to safeguard national security, and protect public interests of the entire society.
第二條　本法之主管機關為行政院。	Article 2. The competent authority over the Act is the Executive Yuan.
第三條　本法用詞，定義如下： 一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。 三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。 四、資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。 五、公務機關：指依法行使公權力之中央、地方機關（構）或	Article 3. The terms under the Act are defined as follows: 1. Information and communication system: That refers to the system to be used to collect, control, transmit, store, circulate, delete information or to make other processing, using and sharing of such information. 2. Information and communication service: That refers to the service to be used to collect, control, transmit, store, circulate, delete information or to make other processing, use and sharing of such information. 3. Cyber security: That refers to such effort to prevent information and communication system or information from being unauthorized access, use, control, disclosure, damage, alteration, destruction or other infringement to assure the confidentiality, integrity and availability of information and system. 4. Cyber security incident: That refers to an event where the state of the system, service or network ,through identification, likely shows violation of the cyber security

公法人。但不包括軍事機關及情報機關。 六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 七、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。 八、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關指定，並報主管機關核定者。 九、政府捐助之財團法人：指其營運及資金運用計畫應依預算法第四十一條第三項規定送立法院，及其年度預算書應依同條第四項規定送立法院審議之財團法人。	policy, or failure of the security protective measures, thus adversely affect performance of information and communication system function, and constitute a threat against the cyber security policy. 5. Government agency: That refers to central, local government agency (institution) or public juristic person that exercises public power according to law, excluding military and intelligence agency. 6. Specific non-government agency: That refers to critical infrastructure provider, government-owned enterprises and government-endowed foundation. 7. Critical infrastructure: That refers to asset, system or network, either physical or virtual, once discontinued from operation or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizen and economic activities. Which shall be re-examined and promulgated by the competent authority regularly. 8. Critical infrastructure provider: That refers to the ones who maintain or provide critical infrastructure either in whole or in part, as designated by the central authority in charge of relevant industry, which shall be submitted to the competent authority for ratification. 9. Government-endowed foundation: That refers to a foundation of which the operation and capital employment plan of its funds shall be submitted to the Legislative Yuan in accordance with Paragraph 3 of Article 41 of the Budget Act and its annual budget statement shall be submitted to the Legislative Yuan for deliberation in

	accordance with Paragraph 4 of the same Article.
第四條　為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項： 一、資通安全專業人才之培育。 二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。 三、資通安全產業之發展。 四、資通安全軟硬體技術規範、相關服務與審驗機制之發展。 前項相關事項之推動，由主管機關以國家資通安全發展方案定之。	Article 4. In an effort to promote cyber security, the government shall provide resources, and integrate the momentum of both civilian groups and private sectors, and boost cyber security awareness of all people, and implement the following issues: 3. Cultivation of cyber security professionals. 4. Cyber security technology research and development, integration, application, and industry-academia cooperation, as well as interchange and cooperation with international community. 5. Development of cyber security industry. 6. Development of cyber security related software and hardware specifications, relevant services and verification mechanism. Issues Promotion in the preceding Paragraph shall be stipulated by the competent authority under the national cyber security program.
第五條　主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。 前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。	Article 5. The competent authority shall plan and promote the cyber security policy, and the cyber security technology development, and interchange and cooperation with international community, and the comprehensive cyber security protection relevant undertakings, as well as announce the report of national cyber security status, the summary auditing report on the implementation of the cyber security maintenance plan for the government agency, and the national cyber security program. The status report, summary auditing report and the national cyber security programs of the preceding Paragraph shall be submitted to the Legislative Yuan for review.
第六條　主管機關得委任或委託其他公務機關、法人或團體，辦理	Article 6. The competent authority may commission or entrust other government agency,

資通安全整體防護、國際交流合作及其他資通安全相關事務。 前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉關鍵基礎設施提供者之秘密。	juristic person or organization to implement integrated protection of cyber security, interchange and cooperation with international community, and other cyber security related issues. The government agency, juristic person or organization, or second-tier subcontractor of the preceding Paragraph shall not divulge the secret of critical infrastructure provider which becomes known in the process of enforcement or implement of relevant issues.
第七條 主管機關應衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主管機關定之。 主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。 特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。	Article 7. The competent authority shall stipulate the cyber security responsibility levels by considering the criteria on the importance, confidentiality and sensitivity of the business, the hierarchy of the agency, and the category, quantity and attribute of the information reserved or processed, as well as the scale and attribute of the information and communication system of the government agency and specific non-government agency. The relevant regulations regard the baseline for responsibility levels, application for a change in the level, content of obligation, staffing of dedicated personnel and other regulations and issues concerned shall be stipulated by the competent authority. The competent authority may audit a specific non-government agency in its implementation of cyber security maintenance plan, of which the frequency, content, method and other issues concerned shall be stipulated by the competent authority. A specific non-government agency is audited as per preceding Paragraph, and found defective or needing improvement in the cyber security maintenance program, it shall submit the improvement report to the competent authority and to the central authority in charge of relevant

	industry.
第八條　主管機關應建立資通安全情資分享機制。 　前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。	Article 8. The competent authority shall set up the cyber security information sharing mechanism. Regulation regarding analysis, integration, and the sharing of content, procedure and method, and other matters of the cyber security information in the preceding Paragraph shall be stipulated by the competent authority.
第九條　公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。	Article 9. A government agency or specific non-government agency outsources for setup, maintenance of the cyber security system, or for provision of cyber security services, such government agency or specific non-government agency shall, within the realm of this Act, take into account outsourced party's professional capability and hands-on experience, as well as attribute of the outsourced item and requirement of cyber security, select the appropriate party for outsourcing and oversee its cyber security maintenance service.
第二章　公務機關資通安全管理	Chapter II. Government Agency Cyber Security Management
第十條　公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。	Article 10. A government agency shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.
第十一條　公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。	Article 11. A government agency shall staff the position of Cyber Security Officer, which to be concurrently served by the deputy head or other appropriate personnel as designated by the agency head. The Cyber Security Officer shall assume the responsibility to carry out and oversee the cyber security business of the agency.
第十二條　公務機關應每年向上級	Article 12. A government agency shall submit to

或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。	the superior or supervisory authority about the implementation of the cyber security maintenance plan annually. Without such superior authority, the implementation report of the cyber security maintenance program shall be submitted to the competent authority.
第十三條　公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。	Article 13. A government agency shall audit the subordinate authority under its supervision about the implementation of the cyber security maintenance plan. When an agency is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the auditing agency and the superior or the supervisory authority.
第十四條　公務機關為因應資通安全事件，應訂定通報及應變機制。 公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。 公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。	Article 14. To cope with cyber security incident, a government agency shall stipulate the reporting and responding mechanism. When privy to a cyber security incident, the government agency shall report to the superior or supervisory authority as well as to the competent authority. Without such superior authority, the government agency shall report to the competent authority. A government agency shall file a report on the investigation, handling and improvement on the cyber security incident, and shall submit the report to the superior or supervisory authority as well as the competent authority. Without a superior authority, the government agency shall submit to the competent authority. Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority.
第十五條　公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。	Article 15. Personnel with proven performance in cyber security maintenance, a government

前項獎勵事項之辦法，由主管機關定之。	agency shall present incentive award. Regulations for such incentive award in the preceding Paragraph shall be stipulated by the competent authority.
第三章　特定非公務機關資通安全管理	Chapter III. Specific Non-Government Agency Cyber Security Management
第十六條　中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。 關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。 關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。 中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。 關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關。 第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。	Article 16. The central authority in charge of relevant industry shall, after consulting with the relevant government agency, civil associations, scholars and experts for their opinions, designate the critical infrastructure provider and submit to the competent authority for approval, while notifying the approved provider in writing. A critical infrastructure provider shall satisfy the requirements of the cyber security responsibility level , and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan. A critical infrastructure provider shall submit to the central authority in charge of relevant industry about the implementation of the cyber security maintenance plan. The central authority in charge of relevant industry shall audit the critical infrastructure provider about the implementation of the cyber security maintenance plan. When a critical infrastructure provider is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the central authority in charge of relevant industry. Regulations regarding the essentials of the

	cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in Paragraph 2 to Paragraph 5 shall be drafted by the central authority in charge of relevant industry, and submit to the competent authority for approval.
第十七條　　關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。 中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。 中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。 前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。	Article 17. A specific non-government agency other than critical infrastructure provider, shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan. The central authority in charge of relevant industry may request the specific non-government agency under their charge mentioned in the preceding Paragraph, to submit a report about implementation of the cyber security maintenance plan. The central authority in charge of relevant industry may audit the specific non-government agency under their charge mentioned in the Paragraph 1 regarding their implementation of the cyber security maintenance plan. When found defective or needing improvement in the cyber security maintenance plan, the audited specific non-government agency shall be required to submit an improvement report before a specified date. Regulations regarding the essentials of the cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in preceding three

	Paragraphs shall be drafted by the central authority in charge of relevant industry, and submit to the competent authority for approval.
第十八條　　特定非公務機關為因應資通安全事件，應訂定通報及應變機制。 特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。 特定非公務機關應向中央目的事業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由主管機關定之。 知悉重大資通安全事件時，主管機關或中央目的事業主管機關於適當時機得公告與事件相關之必要內容及因應措施，並得提供相關協助。	Article 18. To cope with cyber security incident, a specific non-government agency shall stipulate the reporting and responding mechanism. When privy to a cyber security incident, a specific non-government agency shall report to the central authority in charge of relevant industry. A specific non-government agency shall file a report on the investigation, handling and improvement on the cyber security incident and shall submit the report to the central authority in charge of relevant industry. In case of a severe cyber security incident, it shall further notify the competent authority. Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority. When privy to a severe cyber security incident, the competent authority or the central authority in charge of relevant industry may, in a timely manner, promulgate the essential contents of the incident and coping measures and render relevant support.
第四章　罰則	Chapter IV. Penalties
第十九條　公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。 前項懲處事項之辦法，由主管機關定之。	Article 19. Personnel of a government agency shall be subject to discipline or penalty in accordance with the relevant regulations if failing to comply with the regulation of the Act. Regulations for such penalty in the preceding Paragraph shall be stipulated by the competent authority.

第二十條　特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰：	Article 20. If a specific non-government agency has one among those enumerated below transpired, the central authority in charge of relevant industry shall order it to complete corrective actions within the specified time limit. If it fails to complete corrective actions within the specified time limit, it shall be subject to a fine ranging from NT$100,000 as the minimum to NT$1,000,000 as the maximum for each offense:
一、未依第十六條第二項或第十七條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫必要事項之規定。	1. If it fails to stipulate, amend or implement the cyber security maintenance plan in accordance with Paragraph 2 of Article 16 or Paragraph 1 of Article 17, or violates the essential items in the cyber security maintenance plan under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.
二、未依第十六條第三項或第十七條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫實施情形提出之規定。	2. If it fails to submit the report on implementation of the cyber security maintenance plan to the central authority in charge of relevant industry in accordance with Paragraph 3 of Article 16 or Paragraph 2 of Article 17, or fails the requirements with the submittal of the implementation of the cyber security maintenance plan stipulated under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.
三、未依第七條第三項、第十六條第五項或第十七條第三項規定，提出改善報告送交主管機關、中央目的事業主管機關，或違反第十六條第六項或第十七條第四項所定辦法中有關改善報告提出之規定。	3. If it fails the requirements under Paragraph 3 of Article 7, Paragraph 5 of Article 16 or Paragraph 3 of Article 17, unable to submit the improvement reports to the competent authority, the central authority in charge of relevant industry, or violates the regulation with the submitting of the improvement report under Paragraph 6 of Article 16 or Paragraph 4 of Article 17.
四、未依第十八條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十八條第四項所定辦法中有關通報及應變機制必要事項之規定。	4. If it fails to stipulate the reporting and

五、未依第十八條第三項規定，向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告，或違反第十八條第四項所定辦法中有關報告提出之規定。 六、違反第十八條第四項所定辦法中有關通報內容之規定。	responding mechanism of cyber security incident in accordance with Paragraph 1 of Article 18, or violates the essential items in the reporting and responding mechanism under Paragraph 4 of Article 18. 5. If it fails the requirements under Paragraph 3 of Article 18, unable to submit the cyber security investigation, handling and improvement reports regarding cyber security incidents to the central authority in charge of relevant industry or the competent authority, or violate the regulation with the submitting of the report under Paragraph 4 of Article 18. 6. If it violates the regulation regarding the contents of notification under Paragraph 4 of Article 18.
第二十一條　特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。	Article 21. A specific non-government agency violates the provisions Paragraph 2 of Article 18, by failing to report a cyber security incident, the central authority in charge of relevant industry shall impose a fine ranging from NT$300,000 as the minimum to NT$5,000,000 as the maximum, and shall order it to complete improvement within a specified time limit. If it fails to complete such requirement within the specified time limit, a penalty for each additional offense shall be re-imposed.
第五章 附則	Chapter V.　Supplementary provisions
第二十二條　本法施行細則，由主管機關定之。	Article 22. The enforcement rules of the Act shall be stipulated by the competent authority.
第二十三條　本法施行日期，由主管機關定之。	Article 23. The implementation date of the Act shall be stipulated by the competent authority.

資通安全管理法施行細則-英譯對照

資通安全管理法施行細則	Enforcement Rules of Cyber Security Management Act
第一條　本細則依資通安全管理法（以下簡稱本法）第二十二條規定訂定之。	Article 1 These Rules are stipulated in accordance with Article 22 of the Cyber Security Management Act (hereinafter referred to as the Act).
第二條　本法第三條第五款所稱軍事機關，指國防部及其所屬機關（構）、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款及第二項規定之機關。	Article 2 The term “military agency” as used in Subparagraph 5 of Article 3 of the Act refers to the Ministry of National Defense and its subordinate agency (institution), troop, school; and the term “intelligence agency” as used therein, refers to the agency specified in Subparagraph 1 of Paragraph 1 and Paragraph 2 of Article 3 of the National Intelligence Services Law.
第三條　公務機關或特定非公務機關（以下簡稱各機關）依本法第七條第三項、第十三條第二項、第十六條第五項或第十七條第三項提出改善報告，應針對資通安全維護計畫實施情形之稽核結果提出下列內容，並依主管機關、上級或監督機關或中央目的事業主管機關指定之方式及時間，提出改善報告之執行情形： 十、缺失或待改善之項目及內容。 十一、發生原因。 十二、為改正缺失或補強待改善項目所採取管理、技術、人力或資源等層面之措施。 十三、前款措施之預定完成時程及執行進度之追蹤方式。	Article 3 In submitting improvement reports under Paragraph 3 of Article 7, Paragraph 2 of Article 13, Paragraph 5 of Article 16 or Paragraph 3 of Article 17 of the Act, the government agency or the specific non-government agency (hereinafter referred to as “each agency”) shall submit the following contents in response to the audit result of the implementation –of the cyber security maintenance plan, and shall submit the implementation of the improvement report in the manner and within the time as designated by the competent authority, superior or supervisory authority, the central authority in charge of relevant industry: 1. Flaws or items to be improved. 2. Causes of occurrence. 3. Measures in aspects of management, technology, manpower, or resource to be taken for flaws or items to be improved. 4. The estimated completion schedules of the measures under the preceding subparagraph and the tracking method on implementation progresses.
第四條　各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業	Article 4 When each agency outsources parties for setup, maintenance of information and communication system, or provision of information and

務），選任及監督受託者時，應注意下列事項： 一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。 二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。 三、受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。 四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。 五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。 六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。 七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。 八、受託者應採取之其他資通安全相關維護措施。 九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他	communication service (hereinafter referred to as the “outsourced business”) in accordance with Article 9 of the Act, attention should be paid to the following matters for the selection and supervision of the outsourced party. 1. The procedures and environment of the outsourced party in conducting outsourced business shall have completed cyber security management measures or have passed the verification of third party. 2. The outsourced party shall deploy sufficient and properly qualified and trained cyber security professionals who hold cyber security professional licenses or have similar business experience. 3. Whether the outsourced party can second-tier subcontract outsourced business’ scopes and objects that may be second-tier subcontract and the cyber security maintenance measures that the second-tier subcontractor should have. 4. If the outsourced business involves classified national security information, the person who conduct the outsourced business shall be reviewed and the departure shall be controlled in accordance with the Classified National Security Information Protection Act. 5. If the outsourced business includes customized development of information and communication system , the outsourced party shall provide security testing certificate of such information and communication system; if such information and communications system is the core system of the outsourcing agency, or the outsourcing amount exceeds NT$10,000,000, the outsourcing agency shall conduct itself or contract third party to conduct the security testing; if the use of system or resource other than those developed by the outsourced party is involved, content and source of those not developed by the outsourced party shall be indicated and the certification of authorization thereof shall be

適當方式確認受託業務之執行情形。 委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項： 一、曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。 二、曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。 三、曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。 四、其他與國家機密保護相關之具體項目 第一項第四款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。	provided. 6. If the outsourced party conducts outsourced businesses in violation of the relevant regulatory requirement of cyber security or becomes aware of cyber security incident, it shall immediately notify the outsourcing agency thereof and take remedy measure therefor. 7. If the entrusting relationship is terminated or canceled, it shall be confirmed that the outsourced party has returned, handed over, deleted or destroyed all materials in its possession for the performance of the contract. 8. The outsourced party shall take other relevant measure for cyber security. 9. The outsourcing agency shall, periodically, or whenever it becomes aware of the occurrence of cyber security incident of the outsourced party that might affect the outsourced business, confirm the implementation status of the outsourced business by audit or other appropriate method. In conducting the competency audit under Subparagraph 4 of the preceding paragraph, the outsourcing agency shall take into consideration the confidential level and content of the classified national security information in which the outsourced business is involved, and shall, to the necessary extent, check whether the personnel of the outsourced party who performs such business or other personnel who might access such classified national security information has any of the following circumstances: 1. One who had committed the offense of disclosing secret, or had committed the offense of civil disturbance or treason after the termination of the Period of National Mobilization in Suppression of Communist Rebellion, and was finally convicted, or was put on a wanted list which has not been closed. 2. One who was a former public official, was subject to administrative penalty or demerit record due to a

	violation of relevant regulatory for security confidentiality. 3. One who was induced or coerced by foreign government, mainland China, Hong Kong or Macau government to engage in activity unfavorable to national security or significant interest of the nation. 4. Other concrete item relating to the protection of classified national security information. The circumstance under Subparagraph 4 of Paragraph 1 shall be stated in the tender notice, tender document and contract; before the verification of the competency audit, the relevant personnel shall agree in writing document.
第五條　前條第三項及本法第十六條第一項之書面，依電子簽章法之規定，得以電子文件為之。	Article 5 The “in writing” document under Paragraph 3 of the preceding article and Paragraph 1 of Article 16 of the Act may be the electronic one in accordance with the Electronic Signatures Act.
第六條　本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項： 一、核心業務及其重要性。 二、資通安全政策及目標。 三、資通安全推動組織。 四、專責人力及經費之配置。 五、公務機關資通安全長之配置。 六、資通系統及資訊之盤點，並標示核心資通系統及相關資產。 七、資通安全風險評估。 八、資通安全防護及控制措施。 九、資通安全事件通報、應變及演練相關機制。 十、資通安全情資之評估及因應機制。 十一、資通系統或服務委外辦理之管理措施。 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。 十三、資通安全維護計畫與實施情形之持續精進及績效管理機	Article 6　The cyber security maintenance plan under Article 10, Paragraph 2 of Article 16, and Paragraph 1 of Article 17 of the Act shall include the following: 1. Core businesses and their significance. 2. Cyber security policy and objectives. 3. The organization promoting cyber security. 4. The deployment of dedicated manpower and fund. 5. The deployment of Cyber Security Officer of the government agency. 6. The inventory of information and communication systems and information, and indicating the core ones and relevant assets. 7. Risk assessments of cyber security. 8. Protection and control measures for cyber security. 9. The notification, response and rehearsal mechanisms relating to cyber security incidents. 10. Cyber security information assessment and response mechanism. 11. Management measures for outsourced information and communication system or service.

制。 各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括前項各款之執行成果及相關說明。 第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關經其上級或監督機關同意，得由其上級、監督機關或其上級、監督機關所屬公務機關辦理；特定非公務機關經其中央目的事業主管機關同意，得由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關或中央目的事業主管機關所管特定非公務機關辦理。	12. Assessment mechanism for personnel of the government agency who conducts business involving cyber security matters. 13. The continual improvement and performance management mechanism for the cyber security maintenance plan and implementation status. The implementation of cyber security maintenance plans submitted by each agency under Article 12, Paragraph 3 of Article 16, or Paragraph 2 of Article 17 of the Act shall include the implementation results of and relevant explanations for those under each subparagraph of the preceding paragraph. The stipulation, amendment, and implementation of the cyber security maintenance plans under Paragraph 1, and the submission of the implementation thereof to be conducted by a government agency may, with consent of its superior or supervisory authority, be conducted by its superior or supervisory authority or another government agency subordinate to its superior or supervisory authority; and in case of a specific non-government agency, the same may, with consent of its central authority in charge of relevant industry, be conducted by its central authority in charge of relevant industry, a subordinate government agency of such central authority in charge of relevant industry, or another specific non-government agency regulated by the central authority in charge of relevant industry.
第七條　前條第一項第一款所定核心業務，其範圍如下： 一、公務機關依其組織法規，足認該業務為機關核心權責所在。 二、公營事業及政府捐助之財團法人之主要服務或功能。 三、各機關維運、提供關鍵基礎設施所必要之業務。 四、各機關依資通安全責任等級分級辦法第四條第一款至第五款	Article 7　The scope of the core businesses specified in Subparagraph 1 of Paragraph 1 of the preceding article are as follows: 1. Businesses that are considered as the core accountabilities of the government agency as determined by its organizational regulation. 2. Major services or functions of government-owned enterprise and government-endowed foundation. 3. Businesses that are required by each agency for the

或第五條第一款至第五款涉及之業務。 前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。	maintenance and provision of critical infrastructure. 4. Businesses in which each agency is involved in accordance with Paragraphs 1 to 5 of Article 4, or Paragraphs 1 to 5 of Article 5 of the Regulations on Classification of Cyber Security Responsibility Levels. The term “core information and communication system” as used in Subparagraph 6 of Paragraph 1 of the preceding article refers to the system that is necessary for supporting the continual operation of core business, or that is of high level of defense requirements as determined in accordance with Schedule 9 to the Regulations on Classification of Cyber Security Responsibility Levels – principles of classification of cyber system defense requirement levels
第八條　本法第十四條第三項及第十八條第三項所定資通安全事件調查、處理及改善報告，應包括下列事項： 一、事件發生或知悉其發生、完成損害控制或復原作業之時間。 二、事件影響之範圍及損害評估。 三、損害控制及復原作業之歷程。 四、事件調查及處理作業之歷程。 五、事件根因分析。 六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。 七、前款措施之預定完成時程及成效追蹤機制。	Article 8　The investigation, handling and improvement report on cyber security incident under Paragraph 3 of Article 14 and Paragraph 3 of Article 18 of the Act shall include the following: 1. Times of the occurrences of or the awareness of the occurrences of the incidents, the completion of damage control or recovery operations. 2. The scope affected by the incidents and the damage assessment. 3. The courses of damage control and recovery operations. 4. The courses of incident investigations and handling operations. 5. Cause analysis of the incident. 6. Measures in aspects of management, technology, manpower or resources taken to prevent the reoccurrences of similar incident. 7. The estimated completion schedule and the follow-up mechanism of the measures under the preceding subparagraph.
第九條　中央目的事業主管機關依本法第十六條第一項規定指定關鍵基	Article 9　Before designating critical infrastructure providers under Paragraph 1 of Article 16 of the Act,

礎設施提供者前，應給予其陳述意見之機會。	the central authority in charge of relevant industry shall give such providers the opportunity to state their opinions.
第十條　本法第十八條第三項及第五項所稱重大資通安全事件，指資通安全事件通報及應變辦法第二條第四項及第五項規定之第三級及第四級資通安全事件。	Article 10　The term “severe cyber security incident” as used in Paragraphs 3 and 5 of Article 18 of the Act refer to level-3 and level-4 cyber security incidents specified in Paragraphs 4 and 5 of Article 2 of the Regulations on the Notification and Response of Cyber Security Incidents.
第十一條　主管機關或中央目的事業主管機關知悉重大資通安全事件，依本法第十八條第五項規定公告與事件相關之必要內容及因應措施時，應載明事件之發生或知悉其發生之時間、原因、影響程度、控制情形及後續改善措施。 前項與事件相關之必要內容及因應措施，有下列情形之一者，不予公告： 一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或公開有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。 二、其他依法規規定應秘密、限制或禁止公開之情形。 第一項與事件相關之必要內容及因應措施含有前項不予公告之情形者，得僅就其他部分公告之。	Article 11　When the competent authority or the central authority in charge of relevant industry is privy to a cyber security incident and publicize the necessary contents and countermeasures relating to severe cyber security incidents under Paragraph 5 of Article 18 of the Act, upon awareness of such incidents, times of occurrence or privy of the occurrence, causes, affection degree, control status, and subsequent improvement measures of such incidents shall be stated in the publications. Under any of the following circumstances, the necessary contents and contingency measures relating to the incidents under the preceding paragraph shall not be publicized: 1. If it involves trade secrets or information relating to business operations of individuals, juristic persons or organizations or if the disclosure might infringe upon rights or other rightful interests of the government agency, individual, juristic person or organizations; except as is otherwise required by law, or necessary for public welfare or necessary for protection of life, body, and health of people, or with consent of the parties concerned. 2. Other circumstances of confidentiality, restriction, or prohibition on disclosure as required by law. If the necessary contents and contingency measure relating to the incidents shall not be publicized under Paragraph 1, only the other portion may be publicized.

第十二條　特定非公務機關之業務涉及數中央目的事業主管機關之權責者，主管機關得協調指定一個以上之中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。	Article 12　If businesses of the specific non-government agency involve the accountabilities of several central authority in charge of relevant industry, the competent authority may designate via coordination more than one central authority in charge of relevant industry to solely or jointly conduct the matters to be conducted by the central authority in charge of relevant industry under the Act.
第十三條　本細則之施行日期，由主管機關定之。 本細則修正條文自發布日施行。	Article 13　The implementation date of these Rules shall be stipulated by the competent authority. The amendments to these Enforcement Rules shall take effect on the date of promulgation.

資通安全責任等級分級辦法-英譯對照

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定
中華民國 108 年 8 月 26 日行政院院臺護字第 1080184606 號令修正

資通安全責任等級分級辦法	Regulations on Classification of Cyber Security Responsibility Levels
第一條　本辦法依資通安全管理法（以下簡稱本法）第七條第一項規定訂定之。	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”).
第二條　公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。	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.
第三條　主管機關應每二年核定自身資通安全責任等級。 行政院直屬機關應每二年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。 直轄市、縣（市）政府應每二年提交自身、所屬或監督之公務機關，與所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級，報主管機關核定。 直轄市及縣（市）議會、鄉（鎮、市）民代表會及直轄市山地原住民區民代表會應每二年提交自身資通安全責任等級，由其所在區域之直轄市、縣（市）政府彙送主管機關核定。 總統府、國家安全會議、立法院、司法院、考試院及監察院應每二年核定自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，送主管機關備查。 各機關因組織或業務調整，致須變更原資通安全責任等級時，應即依前五項規定程序辦理等級變更；有	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

新設機關時，亦同。 第一項至第五項公務機關辦理資通安全責任等級之提交或核定，就公務機關或特定非公務機關內之單位，認有另列與該機關不同等級之必要者，得考量其業務性質，依第四條至第十條規定認定之。	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 level due to adjustment to organization or business, it shall immediately conduct the change to level 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 level 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 business of such entities.
第四條　各機關有下列情形之一者，其資通安全責任等級為 A 級： 業務涉及國家機密。 業務涉及外交、國防或國土安全事項。 業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。 業務涉及全國性民眾或公務員個人資料檔案之持有。 屬公務機關，且業務涉及全國性之關鍵基礎設施事項。 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。 屬公立醫學中心。	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 authority in charge of relevant 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.
第五條　各機關有下列情形之一	Article 5 The cyber security responsibility levels of

者，其資通安全責任等級為 B 級： 業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理。 業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。 業務涉及區域性或地區性民眾個人資料檔案之持有。 業務涉及中央二級機關及所屬各級機關（構）共用性資通系統之維運。 屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。 屬公立區域醫院或地區醫院。	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.
第六條　各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C 級。 前項所定自行或委外設置之資通系統，指具權限區分及管理功能之資通系統。	Article 6 The cyber security responsibility levels of each agency who maintains and operates by itself or outsources the establishment and development of information and communication system 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.
第七條　各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。	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.
第八條　各機關有下列情形之一者，其資通安全責任等級為 E 級： 無資通系統且未提供資通服務。	Article 8 The cyber security responsibility levels of each agency under any of the following circumstances are Level-E:

屬公務機關，且其全部資通業務由其上級機關、監督機關或上開機關指定之公務機關兼辦或代管。 屬特定非公務機關，且其全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機關，或出資之公務機關兼辦或代管。	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.
第九條　各機關依第四條至前條規定，符合二個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。	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.
第十條　各機關之資通安全責任等級依前六條規定認定之。但第三條第一項至第五項之公務機關提交或核定資通安全責任等級時，得考量下列事項對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級： 業務涉及外交、國防、國土安全、全國性、區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院業務者，其中斷或受妨礙。 業務涉及個人資料、公務機密或其他依法規或契約應秘密之資訊者，其資料、公務機密或其他資訊之數量與性質，及遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害。 各機關依層級之不同，其功能受影響、失效或中斷。 其他與資通系統之提供、維運、規模或性質相關之具體事項。	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, 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.
第十一條　各機關應依其資通安全	Article 11 Each agency shall conduct the matters

責任等級，辦理附表一至附表八之事項。 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；特定非公務機關之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。 各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。 公務機關之資通安全責任等級為A級或B級者，應依主管機關指定之方式，提報第一項及第二項事項之辦理情形。 中央目的事業主管機關得要求所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。	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 information and communication system, it may, with consent of each agency submitting its level under Paragraph 2 to Paragraph 4 of Article 3 or each agency approving its level 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 competent authority will be exempted from execution with consent itself. 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.
第十二條　本辦法之施行日期，由主管機關定之。 本辦法修正條文自發布日施行。	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

附表一

附表一　資通安全責任等級 A 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人；須以專職人員配置之。
	內部資通安全稽核		每年辦理二次。
	業務持續運作演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		每年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
		滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運

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

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the government agency shall inspect the appropriateness of the classification of levels of the information and communication systems at least once a year.
	The importation of the information security management system and verification by an impartial third party		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the government agency shall deploy four persons on full-time basis.
	Internal cyber security audit		Conduct twice a year.
	Business sustainable operation rehearsal		Conduct once a year for all core information and communication systems.
	Cyber security governance maturity assessment		Conduct once a year.
Technical aspect	Security detection	Vulnerability scanning	Conduct twice a year for all core information and communication systems.
		Penetration test	Conduct once a year for all core information and communication systems.
	Cyber security	Inspection of network	Conduct once a year.

			及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。
	政府組態基準		初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。
	資通安全弱點通報機制		初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	端點偵測及應變機制		初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統	

	health diagnosis	frameworks	
		Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of level, the government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof and submit the monitoring management documentation in the manner designated by the competent authority. The monitoring scope shall include the contents conducted for “Endpoint detection and response mechanism” and “Cyber security defense” as specified in this Schedule, the cyber equipment records of the active directory system and the agency’s core information and communication system, and the records of information service or the application.
	Government configuration baseline		Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of government configuration baseline for the items publicized by the competent authority, and shall continue the maintenance and operation thereof.
	Vulnerability alert and		Within one year of receipt of initial approval or change of

		者，應備應用程式防火牆	
		進階持續性威脅攻擊防禦措施	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安 全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		一、初次受核定或等級變更後之一年內，至少四名資通安全專職人員，分別各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內符合規定。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。
二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構；第三方核發之驗證證書應有前開委託機構之認證標誌。
三、資通安全專職人員，指應全職執行資通安全業務者。
四、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。
五、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。
六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。
七、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

	notification system mechanism		levels, the government agency shall complete the import operation of the vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the government agency shall, within one year of the enforcement of the amendments, complete the import operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Endpoint detection and response mechanism		Within two years of receipt of initial approval or change of levels, the government agency shall complete the import operation of endpoint detection and response mechanism, and shall continue the maintenance and operation thereof and submit the detection data in the manner designated by the competent authority. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the government agency shall, within two years of the enforcement of the amendments, complete the endpoint detection and response mechanism, continue the maintenance and operation thereof and submit the detection data in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If the government agency has email servers, it should have email filtering mechanism	

		Intrusion detection and defense mechanism	
		If the government agency has core information and communication systems for external services, it should have the application firewalls	
		Defense measures for advanced persistent threat attacks	
Awareness and training	Cyber security education and training	Full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive general cyber security education training for not less than three hours.
	Cyber security professional license and competence training certificates		1. Within one year after receipt of initial approval or change of levels, at least four full-time cyber security persons shall each hold one or more licenses and certificates, and shall continually maintain the validity of the licenses and certificates. 2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, such requirements shall be met within one year of the

		enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certificate issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.
4. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.
5. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
6. Endpoint detection and response mechanism refers to the protective operations with functions of active scanning and detecting on endpoint, vulnerability protection, analysis of suspicious program or abnormal activities and display function of the level of relevant threats.
7. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.

附表二

附表二 資通安全責任等級 A 級之特定非公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人。
	內部資通安全稽核		每年辦理二次。
	業務持續運作演練		全部核心資通系統每年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
		滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運。其監控範圍應包括本表所定「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服

Schedule 2: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-A

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of the information and communication systems at least once a year.
	The importation of the information security management system and verification by an impartial third party		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the specific non-government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the specific non-government agency shall deploy four persons.
	Internal cyber security audit		Conduct twice a year
	Business sustainable operation rehearsal		Conduct once a year for all core information and communication systems
Technical aspect	Security detection	Vulnerability scanning	Conduct twice a year for all core information and communication systems
		Penetration test	Conduct once a year for all core information and communication systems
	Cyber	Inspection of	Conduct once a year

			務或應用程式紀錄。
	資通安全弱點通報機制		關鍵基礎設施提供者初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
		進階持續性威脅攻擊防禦措施	
認知與訓練	資通安全教育訓練	資通安全專責人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專責人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，至少四名資通安全專責人員，各自持有證

	security health diagnosis	network frameworks	
		Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof. The monitoring scope shall include the contents conducted for “Cyber security defense” as specified in this Schedule, the cyber equipment records of the active directory system and the agency’s core information and communication system, and the records of information service or the application.
	Vulnerability alert and notification system mechanism		Within one year after receipt of initial approval or change of level, the critical infrastructure provider shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.

		照一張以上，並持續維持證照之有效性。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內符合規定。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構；第三方核發之驗證證書應有前開委託機構之認證標誌。

三、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

六、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

			If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the critical infrastructure provider shall, within one year of the enforcement of the amendments, complete the import operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	
		Network firewall	
		If the specific non-government agency has email servers, it should have email filtering mechanism	
		Intrusion detection and defense mechanism	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		If the specific non-government agency has core information and communication systems for external services, it should have the application firewalls	
		Defense measures for advanced	

		persistent threat attacks	
Awareness and training	Cyber security education and training	Dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours
	Cyber security professional licenses		1. Within one year after receipt of initial approval or change of levels, at least four dedicated cyber security persons shall each hold one or more licenses, and shall continually maintain the validity of licenses. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certificate issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by the central authority in charge of relevant industry.
4. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.
6. The central authority in charge of relevant industry of the specific non-government agency may, depending on the

	actual requirements and to the extent of compliance with these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

附表三 資通安全責任等級 B 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；須以專職人員配置之。
	內部資通安全稽核		每年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
	資安治理成熟度評估		每年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點

Schedule 3: Matters to be conducted by the government agency of cyber security responsibility Level-B

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year.
	The importation of the information security management system and verification by an impartial third party		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the government agency shall deploy two persons on full-time basis.
	Internal cyber security audit		Conduct once a year.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
	Cyber security governance maturity assessment		Conduct once a year.
Technical aspect	Security detection	Vulnerability scanning	Conduct once a year for all core information and communication systems.
		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber security	Inspection of network	Conduct once every two years.

			偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。
	政府組態基準		初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。
	資通安全弱點通報機制		初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	端點偵測及應變機制		初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	

	health diagnosis	frameworks	
		Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of level, the government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof and submit the monitoring management documentation in the manner designated by the competent authority. The monitoring scope shall include the contents conducted for “Endpoint detection and response mechanism” and “Cyber security defense” as specified in this Schedule, the cyber equipment records of the active directory system and the agency’s core information and communication system, and the records of information service or the application.
	Government configuration baseline		Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of government configuration baseline for the items publicized by the competent authority, and shall continue the maintenance and operation thereof.
	Vulnerability alert and		Within one year of receipt of initial approval or change of

認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		一、初次受核定或等級變更後之一年內，至少二名資通安全專職人員，分別各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。 二、　本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內符合規定。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構；第三方核發之驗證證書應有前開委託機構之認證標誌。

三、資通安全專職人員，指應全職執行資通安全業務者。

四、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

五、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。

七、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

	notification system mechanism		levels, the government agency shall complete the import operation of the vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the government agency shall, within one year of the enforcement of the amendments, complete the import operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Endpoint detection and response mechanism		Within two years of receipt of initial approval or change of levels, the government agency shall complete the import operation of Endpoint detection and response mechanism, and shall continue the maintenance and operation thereof and submit the detection data in the manner designated by the competent authority. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, the government agency shall, within two years of the enforcement of the amendments, complete the Endpoint detection and response mechanism, and shall continue the maintenance and operation thereof and submit the detection data in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If the government agency has email servers, it should have email filtering mechanism	

		Intrusion detection and defense mechanism	
		If the government agency has core information and communication systems for external services, it should have the application firewalls	
Awareness and training	Cyber security education and training	Full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours
	Cyber security professional license and competence training certificates		1. Within one year after receipt of initial approval or change of levels, at least two full-time cyber security persons shall each hold one or more license(s) and certificate(s), and shall continually maintain those validity. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.

2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent

	authority for the accreditation in accordance with the Standards Act of our country; the certification issued by such third party shall bear the accreditation mark of the above-said commissioned agency. 3. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time. 4. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority. 5. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act. 6. Endpoint detection and response mechanism refers to the protective operations with functions of active scanning and detecting on endpoint, vulnerability protection, analysis of suspicious program or abnormal activities and display function of the level of relevant threats. 7. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.

附表四

附表四 資通安全責任等級 B 級之特定非公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人。
	內部資通安全稽核		每年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運。其監控範圍應包括本表所定「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服

Schedule 4: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-B

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year.
	The importation of the information security management system and verification by an impartial third party		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the specific non-government agency shall continually maintain the validity of its certification.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the specific non-government agency shall deploy two persons.
	Internal cyber security audit		Conduct once a year.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
Technical aspect	Security detection	Vulnerability scanning	Conduct once a year for all core information and communication systems.
		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber security health	Inspection of network frameworks	Conduct once every two years.

			務或應用程式紀錄。
	資通安全弱點通報機制		關鍵基礎設施提供者初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
認知與訓練	資通安全教育訓練	資通安全專責人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專責人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照		一、　初次受核定或等級變更後之一年內，至少二名資通安全專責人員，各自持有證照一張以上，並持續維持證照之有效性。 二、　本辦法中華民國一百十年八月

	diagnosis	Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of levels, the specific non-government agency shall complete the development of threat detection mechanisms, and shall continue the maintenance and operation thereof. The monitoring scope shall include the contents conducted for “Cyber security defense” as specified in this Schedule, the cyber equipment records of the active directory system and the agency’s core information and communication system, and the records of information service or the application.
	Vulnerability alert and notification system mechanism		1. Within one year after receipt of initial approval or change of level, the critical infrastructure provider shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations were enforced on August 23, 2021, the critical infrastructure provider shall, within one year of the enforcement of the amendments, complete the import

		二十三日修正施行前已受核定者，應於修正施行後一年內符合規定。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構；第三方核發之驗證證書應有前開委託機構之認證標誌。

三、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

六、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

			operation of the vulnerability alert and notification system mechanism, continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If the specific non-government agency has email servers, it should have email filtering mechanism	
		Intrusion detection and defense mechanism	
		If the specific non-government agency has core information and communication systems for external services, it should have the application firewalls	
Awareness and training	Cyber security education and training	Dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.

		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional licenses		1. Within one year after receipt of initial approval or change of levels, at least two dedicated cyber security persons shall each hold one or more license(s) and certificate(s), and shall continually maintain those validity. 2. If it has been approved before the enforcement of the amendments to these Regulations on August 23, 2021, such requirements shall be met within one year of the enforcement of the amendments.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the accreditation in accordance with the Standards Act of our country; the certificate issued by such third party shall bear the accreditation mark of the above-said commissioned agency.
3. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by the central authority in charge of relevant industry.
4. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.
6. The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

附表五

附表五 資通安全責任等級 C 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

Schedule 5: Matters to be conducted by the government agency of cyber security responsibility Level-C

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classification of levels of the information and communication systems developed by itself or outsourced according to Schedule 9; subsequently, the government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year. If the system levels are “high”, the government agency shall, within two years of receipt of initial approval or change of levels, complete the control measures specified in Schedule 10.
	The importation of the information security management system		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority, and shall continually maintain the importation thereof.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the government agency shall deploy one person on full-time basis.
	Internal cyber security audit		Conduct once every two years.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
Technical aspect	Security detection	Vulnerability scanning	Conduct once every two years for all core information and communication systems.
		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber security health diagnosis	Inspection of network frameworks	Conduct once every two years.
		Inspection of malicious	

			本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安 全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別持有證照及證書各一張以上，並持續維持證照及證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、資通安全專職人員，指應全職執行資通安全業務者。

三、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

		cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Vulnerability alert and notification system mechanism		1. Within two years after receipt of initial approval or change of level, the government agency shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations on August 23, 2021, the government agency shall, within two years of the enforcement of the amendments, complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If the government	

		agency has email servers, it should have email filtering mechanism	
Awareness and training	Cyber security education and training	Full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than full-time cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional license and competence training certificates		Within one year after receipt of initial approval or change of levels, at least one full-time cyber security personnel shall hold one or more license(s) and certificate(s), and shall continually maintain the validity of the licenses and certificates.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.
2. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.
3. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.
4. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.
5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.

附表六 資通安全責任等級 C 級之特定非公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		關鍵基礎設施提供者初次受核定或等級變更後之二年內，完成資通安全弱

Schedule 6: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-C

System aspect	Items conducted	Sub-items conducted	Contents conducted
Management aspect	Classification of levels and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classifications of levels of the information and communication systems developed by itself or outsourced according to Schedule 9; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year. If the system levels are “high”, the specific non-government agency shall, within two years of receipt of initial approval or change of levels, complete the control measures specified in Schedule 10.
	The importation of the information security management system		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the standards - CNS 27001 or ISO 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority, and shall continually maintain the importation thereof.
	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the specific non-government agency shall deploy one person.
	Internal cyber security audit		Conduct once every two years.
	Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
Technical aspect	Security detection	Vulnerability scanning	Conduct once every two years for all core information and communication systems.
		Penetration test	Conduct once every two years for all core information and communication systems.
	Cyber	Inspection of	Conduct once every two years.

			點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全專責人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專責人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安 全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，至少一名資通安全專責人員持有證照一張以上，並持續維持證照之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

三、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

四、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

	security health diagnosis	network frameworks	
		Inspection of malicious cyber activities	
		Inspection of malicious activities in user terminal computers	
		Inspection of malicious activities in servers	
		Inspection of settings of directory servers and settings of firewall connections	
	Vulnerability alert and notification system mechanism		1. Within two years after receipt of initial approval or change of level, the critical infrastructure provider shall complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority. 2. If it has been approved before the amendments to these Regulations on August 23, 2021, the critical infrastructure provider shall, within two years of the enforcement of the amendments, complete the import operation of vulnerability alert and notification system mechanism, and shall continue the maintenance and operation thereof and submit the inventory data of information assets in the manner designated by the competent authority.
	Cyber security	Anti-virus software	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation

五、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

	defense	Network firewall If the specific non-government agency has email servers, it should have email filtering mechanism	of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
Awareness and training	Cyber security education and training	Dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each year.
		Information personnel other than dedicated cyber security personnel	Each personnel shall receive the cyber security professional program training or the cyber security competence training for not less than three hours every two years and receive general cyber security education training for not less than three hours each year.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional licenses		Within one year after receipt of initial approval or change of levels, at least one dedicated cyber security personnel shall hold one license or more, and shall continually maintain the validity.

Notes:

1.If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the establishment, maintenance or development of such information and communication system.

2. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by central authority in charge of relevant industry.

3. Vulnerability alert and notification system mechanism refers to the operations in combination of the information asset management and vulnerability management, the grasp of overall risk trends, and the assistance to the agency in fulfilment of matters to be conducted for asset inventory and risk assessment under the Act.

4. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority (entity) recognized by the competent authority.

5. The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for

	the cyber security matters to be conducted by its regulated specific non-government agency.

附表七

附表七 資通安全責任等級 D 級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體 網路防火牆	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

Schedule 7: Matters to be conducted by each agency of cyber security responsibility Level-D

System aspect	Items conducted	Sub-items conducted	Contents conducted
Technical aspect	Cyber security defense	Anti-virus software Network firewall	Within one year after receipt of approval or change of levels, each agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
Awareness and training	Cyber security education and training	General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.

Note: The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

附表八

附表八 資通安全責任等級 E 級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

Schedule 8: Matters to be conducted by each agency of cyber security responsibility Level-E

System aspect	Items conducted	Sub-items conducted	Contents conducted
Awareness and training	Cyber security education and training	General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.

Note: The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.

附表九　資通系統防護需求分級原則

防護需求 等級 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

Schedule 9: Principles of classification of levels of defense requirements of information and communication system

Defense requirements Levels Dimension	High	Medium	Common
Confidentiality	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to limited impact on the operation, asset or reputation of the agency.
Integrity	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to limit impact on the operation, asset or reputation of the agency.
Availability	The occurrence of cyber security incident resulting in impact on the information and	The occurrence of cyber security incident resulting in impact on the information and	The occurrence of cyber security incident resulting in impact on the information and

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

	communication system might cause the interruption of access to or use of the information and information and communication system, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	communication system might cause the interruption of access to or use of the information and information and communication system, leading to serious impact on the operation, asset or reputation of the agency.	communication system might cause the interruption of access to or use of the information and information and communication system, leading to limit impact on the operation, asset or reputation of the agency.
Regulatory compliance	The failure to strictly comply with regulatory requirements relating to the establishment or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the personnel of the agencies to be subject to criminal liabilities.	The failure to strictly comply with regulatory requirements relating to the establishment or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the agencies or their personnel to be subject to administrative punishments, disciplines or penalties.	Other status of establishment or operation of information and communication system under relevant regulatory requirements.

	Note: The defense requirement levels of the information and communication system shall be the highest ones as determined in any of the dimensions of confidentiality, integrity, availability and regulatory compliance relating to such systems.

附表十

附表十　資通系統防護基準

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
存取控制	帳號管理	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、應依機關規定之情況及條件，使用資通系統。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。 五、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、遠端存取之來源應為機關已預先定義及管理之存取控制點。 二、等級「普」之所有控制措施。		一、對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取機關內部網

Schedule 10: Defense standards of information and communication system

Defense requirements of systems Level / Control measure Dimension	Contents of the measures	High	Medium	Common
Access control	Account management	6. The agency shall define the idle time or usable duration of each system and the use status and condition of information and communication system. 7. When the permitted idle time prescribed by the agency or usable time is exceeded, the system should automatically logout the users. 8. Use the information and communication system according to the circumstances and conditions prescribed by the agency. 9. Monitor the information and communication system accounts; report to the administrator if any abnormal use by an account is found 10. All control measures for the level of “medium”.	5. The temporary or emergent accounts which have expired should be deleted or prohibited. 6. The idle accounts of information and communication system should be prohibited. 7. Periodically review the application, establishment, revision, activation, suspension and deletion of accounts of information and communication systems. 8. All control measures for the level of “common”.	Establish the account management mechanism, including the procedure for application, establishment, revision, activation, suspension and deletion.
	Least privilege	The principle of least privilege is adopted. The users(or the procures for acts on behalf of users)are granted the authorized access required for the completion of duties only, depending on the duties and business functions of the agency .		No requirement
	Remote access	1. The source of the remote access should be the access control point ad pre-defined and managed by the agency. 2. All control measures for the level of “common”.		5. For each kind of permitted remote access, the authorization should be obtained in advance; the use restriction,

			段或資通系統後臺之連線。 四、應採用加密機制。
事件日誌與可歸責性	記錄事件	一、應定期審查機關所保留資通系統產生之日誌。 二、等級「普」之所有控制措施。	一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。
	日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。	
	日誌處理失效之回應	一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	資通系統於日誌處理失效時，應採取適當之行動。
	時戳及校時	一、系統內部時鐘應定期與基準時間源進行同步。 二、等級「普」之所有控制措施。	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。

			configuration requirement, connection requirement and documentation should be established. 6. The inspection operation of users' privilege should be completed at the server terminal. 7. The remote access to intranet of the agency or the connection to the information and communication system back office should be monitored. 8. Encryption mechanism should be adopted.
Event log and accountability	Record events	3. The log generated by the information and communication system which is retained by the agency should be reviewed periodically. 4. All control measures for the level of "common".	4. Stipulate the time cycle of records in the logs and retention policy and retain the logs for at least six months. 5. Assure that the information and communication system has the function of record of specific events, and determine the specific information and communication system

	日誌資訊之保護	一、定期備份日誌至與原系統外之其他實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對日誌之存取管理，僅限於有權限之使用者。
營運持續計畫	系統備份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。
	系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。		無要求。
識別與鑑別	內部使用者之識別與鑑別	一、對資通系統之存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	
	身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。		一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關

				incidents to be recorded. 6. Should record various functions executed by the administrator account of the information and communication system.
	Content of log record	The log generated by the information and communication system shall include the type of incidents, dates of occurrence, places of occurrence, and the information about the identification of the users relating to the incidents; the single log mechanism should be adopted to assure the consistency of the formats of output, and other relevant information shall be included in accordance with the cyber security policy and requirements of laws and regulations.		
	Storage capacity of the log	Storage capacity required for the log shall be equipped depending on the requirement of the storage of the log.		
	Response to failure in log process	3. Upon occurrence of the event of failure in log process which should be reported immediately as required by the agency, the information and communication system should give warnings to the specific personnel within the timeframes prescribed by the agency. 4. All control measures for the levels of “medium” and “common”.		In case of failure in log process, the information and communication system should take appropriate actions.
	Time stamp and time calibration	3. The internal clock of the system should periodically synchronize with the time cycle specified by the agency and the source of standard times. 4. All control measures for the level of “common”.		The information and communication system should use the internal clock of the system to generate time stamps required for the log, and such time stamps should be able to correspond to Universal Time Coordinated(UTC) or Greenwich Mean Time(GMT).
	Protection of log information	3. Periodically back up the log to the physical system different from the original audit system. 4. All control measures for the	3. Should use the integrity of the hashing or other proper methods to assure the mechanism. 4. All control measures for the level of “common”.	The access management of the log is limited to the users with privileges.

			自建之失敗驗證機制。 四、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。	
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。		
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。	
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。		
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性）進行確認。		
	系統發展生命週期設計階段	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	無要求。	
	系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、系統應具備發生嚴重錯誤時之通知機制。 三、等級「中」及「普」之所有控制措施。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	

		level of “medium”		
Business continuity plan	Backup of system	4. Should take the backup and restore as a part of the testing of the business continuity plan. 5. Should store the important software of the information and communication system and backup of other security related information in the independent facilities or fire cabinets at the place different from the operating systems. 6. All control measures for the level of “medium”.	3. Should periodically test the backup information to verify the reliability of the backup media and the integrity of the information. 4. All control measures for the level of “common”.	3. Set the requirement for tolerable time of information loss of the system. 4. Execute the system source codes and the data backup.
	System rescue	3. Set the requirements for the tolerable time from the interruption of information and communication system to the recovery of service. 4. When the original service interrupts, the service is provided by the rescue equipment or other method in lieu thereof within the tolerable time.		No requirement
Identification and authentication	Identification and authentication of internal users	3. Adopt multiple authentication technologies for the access to the information and communication system. 4. All control measures for the level of “medium” and “common”.	The information and communication system should have the function of identification and authentication of sole agency users(or the program of act on behalf of agency users); common accounts are prohibited.	
	Identity verification management	4. Identity verification mechanism should prevent from the logon by automatic program or the trials of change of password.		7. When using the preset password to login the system, should immediately change

	系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	一、於系統發展生命週期之維運階段，應執行版本控制與變更管理。 二、等級「普」之所有控制措施。	一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統不使用預設密碼。	
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
	獲得程序	開發、測試及正式作業環境應為區隔。	無要求。	
	系統文件	應儲存與管理系統發展生命週期之相關文件。		
系統與通訊保護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證應定期更換。 五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	無要求。	無要求。

		5. The password resetting mechanisms have verified identities of users again, and then send one-time and time-based tokens. 6. All control measures for the level of “common”.	the password after logon. 8. Information relating to identity verification may not be transmitted by plain text. 9. Have the account lockout mechanism; if the identity verification for account logon fails for five times, disallow such account to continue the trial of logon at least within fifteen minutes, or use the failure verification mechanisms built by the agencies themselves. 10. While the password is used to conduct authentication, the least complexity of password should be imposed; and the restriction on the shortest and longest validity of passwords should be imposed. 11. In the event of change of password, at least the password may not be same as those used for previous three times. 12. The measures specified in points 4 and 5 may be conducted for non-internal users according to the regulations formulated by the agencies themselves.
	Authentication information feedback	The information and communication system should shield the information in the course of authentication.	
	Encryption module authentication	When the information and communication systems use the passwords for authentication, such passwords should be encrypted, or stored after hashing process.	No requirement
	Identification or authentication of non-internal users	The information and communication systems should identity and authenticate non-internal users (or the program of act on behalf of agency users).	
Access to systems and services	Requirement phase of system	Confirm the system security requirements (including confidentiality, availability and integrity).	

	資料儲存之安全	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	無要求。	無要求。
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、　　等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。
	資通系統監控	一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二、等級「中」之所有控制措施。	一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無要求。

備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之系統防護基準。

	development life circle			
	Design phase of system development life circle	1. Depending on the system functions and requirements, identify the threats that might impact on the system, to conduct risk analysis and assessment. 2. Feedback the risk assessment results to the screening items of the requirement phase, and submit the revision of security requirements.		No requirement
	Development phase of system development life circle	4. Execute “source code scanning” security testing. 5. The system should have the notification mechanisms when serious error occurs. 6. All control measures for the level of “medium” and “common”.	1. Should practice necessary control measures for the security requirements. 2. Should pay attention to the avoidance of common software vulnerabilities, and practice necessary measures. 3. When errors occur, the user’s pages display short error message and code only, without detailed error message.	
	Testing phase of system development life circle	1. Execute “penetration testing” security testing. 2. All control measures for the level of “medium” and “common”.	Execute “vulnerability scanning” security testing.	
	Deployment and maintenance operation phase of system development life circle	3. In the maintenance operation phase of system development life circle, the version control and change management shall be implemented. 4. All control measures for the level of “common”.		3. Under the deployment environment, should conduct update and fixing of relevant cyber security threats, and close unnecessary services and ports. 4. Not to use preset passwords for information and communication system.
	Outsourcing phase of system development life circle	If the development of the information and communication system is outsourced, the security requirements by level (including confidentiality, availability, integrity) for each phase of system development life circle shall be included in the outsourcing contract.		
	Obtaining programs	Development, testing, and formal operation environments should be separated.		No requirement
	System documents	Should store the documents relating to the management system development life circle.		
Protection of systems and communications	Confidentiality and integrity of transmission	6. The information and communication system should adopt encryption mechanism, to prevent from unauthorized disclosure of information or to detect the change of information; unless there are substitutive physical	No requirement	No requirement

		protection measures in the course of transmission. 7. Use public, international institution verified and not cracked algorithms. 8. Support the maximum length key of algorithms. 9. Periodically change the encryption key or certification. 10. Should formulate the management regulations on the custody of key at server terminal, and implement security defense measures that should exist.		
	Securities of data storage	The important configuration setting file of the information and communication system and other relevant confidential information required for protection should be encrypted or stored by other appropriate method.	No requirement.	No requirement.
Integrity of systems and information	Vulnerability fixing	3. Periodically confirm the status of fixing of relevant vulnerabilities of the information and communication system. 4. All control measures for the level of “common”.		The vulnerability fixing of the system should be tested for the effectiveness and potential impact, and should be updated periodically.
	Monitoring of information and communication system	3. The information and communication system should adopt automatic tools to monitor the access communication flows; if unusual or unauthorized activities are found, conduct the analysis of such activity. 4. All control measures for the level of “medium”.	3. Monitor the information and communication system to detect the attack and unauthorized connection and to identify the unauthorized users of the information and communication system. 4. All control measures for the level of “common”.	If a sign of hacking to the information and communication system is found, should notify the specific personnel of the agencies thereof.
	The integrity of software and information	3. Should conduct the inspection of the integrity of software and information.	4. Use the integrity verification tools to detect the unauthorized change	No requirement

		4. All control measures for the level of "medium".	of specific software and information. 5. The examination of the legitimacy of input data of users should be placed on the server terminal of the application system. 6. If any violation to the integrity is found, the information and communication system should implement the security defense measures designated by the agency.	

Notes: The central authority in charge of relevant industry of the specific non-government agency may, depending on the actual requirements and to the extent of compliance with these Regulations, otherwise provide for the information and communication system defense standards of its regulated specific non-government agency.

資通安全事件通報及應變辦法_英譯對照

資通安全事件通報及應變辦法	Regulations on the Notification and Response of Cyber Security Incident
第 一 章 總則	Chapter 1 General Provisions
第一條　本辦法依資通安全管理法（以下簡稱本法）第十四條第四項及第十八條第四項規定訂定之。	Article 1 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").
第二條 資通安全事件分為四級。 公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件： 一、非核心業務資訊遭輕微洩漏。 二、非核心業務資訊或非核心資通系統遭輕微竄改。 三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。 各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件： 一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。 二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。 三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。 各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件： 一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。 二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關	Article 2 Cyber security incident is classified into four levels. 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: 1. Minor breach of non-core business information. 2. Minor alteration of non-core business information or non-core information and communication system. 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. The cyber security incident occurred to each agency under any of the following circumstances is the level-2 cyber security incident: 1. Serious breach of non-core business information or minor breach of core business information not involving the maintenance and operation of critical infrastructures. 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. 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

鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。 三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。 各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件： 一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。 二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。 三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。	infrastructures, which may be recovered within tolerable interruption time. The cyber security incident occurred to each agency under any of the following circumstances is the level-3 cyber security incident: 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. 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. 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. 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.
第三條 資通安全事件之通報內容，應包括下列項目： 一、發生機關。 二、發生或知悉時間。 三、狀況之描述。 四、等級之評估。 五、因應事件所採取之措施。 六、外部支援需求評估。 七、其他相關事項。	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.
第 二 章 公務機關資通安全事件之通報及應變	Chapter 2 The notification and response of cyber security incident of government agency
第四條 公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。 前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。 公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。 公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。	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.

第五條　主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級： 一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。 二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，完成資通安全事件之通報後，依前項規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級。 前項機關依規定完成資通安全事件等級之審核後，應於一小時內將審核結果通知主管機關，並提供審核依據之相關資訊。 總統府、國家安全會議、立法院、司法院、考試院、監察院及直轄市、縣（市）議會，應於其自身完成資通安全事件之通報後，依第一項規定時間完成該資通安全事件等級之審核，並依前項規定通知主管機關及提供相關資訊。 主管機關接獲前二項之通知後，應依相關資訊，就資通安全事件之等級進行覆核，並得依覆核結果變更其等級。但主管機關認有必要，或第二項及前項之機關未依規定通知審核結果時，得就該資通安全事件逕為審核，並得為等級之變更。	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.
第六條　公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜： 一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。 二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。 公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。 前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。 上級、監督機關或主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。	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.
第七 條 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，就所屬、監督、所轄或業務相關之公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。 主管機關就公務機關執行資通安全事件之應變作業，得視情形提供必要支援或協助。 公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。	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.
第八 條　總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關及前開鄉（鎮、市）、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。 前項演練作業之內容，應至少包括下列項目： 一、每半年辦理一次社交工程演練。 二、每年辦理一次資通安全事件通報及應變演練。 總統府與中央一級機關及直轄市、縣（市）議會，應依前項規定規劃及辦理資通安全演練作業。	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.
第九條 公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項： 一、判定事件等級之流程及權責。 二、事件之影響範圍、損害程度及機關因應能力之評估。 三、資通安全事件之內部通報流程。 四、通知受資通安全事件影響之其他機關之方式。 五、前四款事項之演練。 六、資通安全事件通報窗口及聯繫方式。 七、其他資通安全事件通報相關事項。	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.
第十條 公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項： 一、應變小組之組織。 二、事件發生前之演練作業。 三、事件發生時之損害控制機制。 四、事件發生後之復原、鑑識、調查及改善機制。 五、事件相關紀錄之保全。 六、其他資通安全事件應變相關事項。	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.
第 三 章 特定非公務機關資通安全事	Chapter 3 The notification and response of cyber security incident of the specific non-

件之通報及應變	government agency
第十一條 特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。 前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。 特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。 特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。	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.
第十二條 中央目的事業主管機關應於特定非公務機關完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級： 一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。 二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。 中央目的事業主管機關依前項規定完成資通安全事件之審核後，應依下列規定辦理： 一、審核結果為第一級或第二級資通安全事件者，應定期彙整審核結果、 依據及其他必要資訊，依主管機關指定之方式送交主管機關。 二、審核結果為第三級或第四級資通安全事件者，應於審核完成後一小時內，將審核結果、依據及其他必要資訊，	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

依主管機關指定之方式送交主管機關。 主管機關接獲前項資料後，得就資通安全事件之等級進行覆核，並得為等級之變更。	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.
第十三條 特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜： 一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。 二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。 特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。 前項調查、處理及改善報告送交之時限，得經中央目的事業主管機關同意後延長之。 中央目的事業主管機關就第一項之損害控制或復原作業及第二項送交之報告，認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。 特定非公務機關就第三級或第四級資通安全事件送交之調查、處理及改善報告，中央目的事業主管機關應於審查後送交主管機關；主管機關就該報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。	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.
第十四條 中央目的事業主管機關就所管特定非公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。 主管機關就特定非公務機關執行資通安全事件應變作業，得視情形提供必要支援或協助。 特定非公務機關知悉第三級或第四級資通安全事件後，應召開會議研商相關事宜。	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.
第十五條 特定非公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項： 一、判定事件等級之流程及權責。 二、事件之影響範圍、損害程度及機關因應能力之評估。 三、資通安全事件之內部通報流程。 四、通知受資通安全事件影響之其他機關之時機及方式。 五、前四款事項之演練。 六、資通安全事件通報窗口及聯繫方式。 七、其他資通安全事件通報相關事項。	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.
第十六條 特定非公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項： 一、應變小組之組織。 二、事件發生前之演練作業。 三、事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或其他必要協助之機制。 四、事件發生後之復原、鑑識、調查及改善機制。 五、事件相關紀錄之保全。 六、其他資通安全事件應變相關事項。	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.
第 四 章 附則	Chapter 4 Supplementary Provisions
第十七條 主管機關就各機關之第三級或第四級資通安全事件，得召開會議，邀請相關機關研商該事件之損害控制、復原及其他相關事宜。	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.
第十八條 公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目： 一、社交工程演練。 二、資通安全事件通報及應變演練。 三、網路攻防演練。 四、情境演練。 五、其他必要之演練。	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.
第十九條 特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目： 一、網路攻防演練。	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:

二、情境演練。 三、其他必要之演練。 主管機關規劃、辦理之資通安全演練作業，有侵害特定非公務機關之權利或正當利益之虞者，應先經其書面同意，始得為之。 前項書面同意之方式，依電子簽章法之規定，得以電子文件為之。	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.
第二十條　公務機關於本辦法施行前，已針對其自身、所屬或監督之公務機關或所管之特定非公務機關，自行或與其他機關共同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬或監督之公務機關或所管之特定非公務機關繼續依該機制辦理資通安全事件之通報及應變。 前項通報及應變機制如有變更，應送主管機關重為核定。	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.
第二十一條 本辦法之施行日期，由主管機關定之。 本辦法修正條文自發布日施行。	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.

特定非公務機關資通安全維護計畫實施情形稽核辦法-英譯對照

特定非公務機關資通安全維護計畫實施情形稽核辦法	Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency
第一條　本辦法依資通安全管理法第七條第二項規定訂定之。	Article 1 These Regulations are stipulated in accordance with Paragraph 2 of Article 7 of the Cyber Security Management Act.
第二條　本辦法所定書面，依電子簽章法之規定，得以電子文件為之。	Article 2 These Regulations stipulate “in writing” document may be an electronic document in accordance with the provisions of the Electronic Signatures Act.
第三條　主管機關除因不可抗力因素外，應每年擇定受稽核之特定非公務機關(以下簡稱受稽核機關)，並以現場實地稽核之方式，稽核其資通安全維護計畫實施情形。 主管機關擇定前項受稽核機關時，應綜合考量其業務之重要性與機敏性、資通系統之規模與性質、資通安全事件發生之頻率與程度、資通安全演練之成果、歷年受主管機關或中央目的事業主管機關稽核之頻率與結果或其他與資通安全相關之因素。 主管機關為辦理第一項稽核，應訂定稽核計畫，其內容包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及中央目的事業主管機關協助事項。 主管機關決定前項稽核之重點領域與基準及項目時，應綜合考量我國資通安全政策、國內外資通安全趨勢、過往稽核計畫之內容	Article 3 Except for cause by force majeure, the competent authority shall select and determine the specific non-government agencies (hereinafter referred to as the “audited agency”), and may audit the implementation of their cyber security maintenance plans through onsite audit every year. In selecting and determining the audited agencies under the preceding paragraph, the competent authority shall give comprehensive consideration to the significance and confidential sensitivities of its businesses, the size and nature of their cyber systems, the frequencies and degrees of occurrence of cyber security incidents, the results of cyber offense and defense exercise, the frequencies and results of audits conducted by the competent authority or the central authority in charge of the relevant industry over past years, or other factors relating to cyber security. In conducting the audit under Paragraph 1, the competent authority shall establish the audit program, the content of which shall include the basis and purposes, time period, essential fields of the audit, the manner of formation of the audit team, confidentiality obligation, the method, standards and items of the audit, and assistance

與稽核結果，及其他與稽核資源之適當分配或稽核成效相關之因素。	issues from the central authority in charge of relevant industry. In determining the essential fields, standards and items of the audit under the preceding paragraph, the competent authority shall take into comprehensive consideration the cyber security policy of our country, domestic and foreign cyber security trends, the contents and results of past audit programs, and any other factors relating to the proper allocation of audit resources or audit effectiveness.
第四條　主管機關辦理前條第一項之稽核，應將稽核計畫於一個月前以書面通知受稽核機關。 受稽核機關如因業務因素或有其他正當理由，得於收受前項通知後五日內，以書面敘明理由向主管機關申請調整稽核日期。 前項申請，除有不可抗力之事由外，以一次為限。	Article 4　In conducting the audit under Paragraph 1of the preceding article, the competent authority shall deliver the audit program notice in writing to the audited agency one month before the audit. Due to business factor or other justifiable reason, the audited agency may apply to the competent authority for adjustment of the audit date within five days of the receipt of the preceding notice in writing. The preceding application is limited to one time except for the case of force majeure.
第五條　主管機關辦理第三條第一項之稽核，得要求受稽核機關為資通安全維護計畫實施情形之說明、協力或提出相關之文件、證明資料供現場查閱，並執行下列事項，受稽核機關及其所屬人員應予配合： 一、稽核前訪談。 二、現場實地稽核。 受稽核機關依法律有正當理由，未能為前項說明、協力或提出資料供現場查閱者，應以書面敘明理由，向主管機關提出。 主管機關收受前項書面後，應進行審核，依下列規定	Article 5　In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the audited agency to give explanations on, to collaborate the implementation of cyber security maintenance plan, or provide relevant documents and supporting information for onsite inspection, and conduct the following issues. The audited agency and its personnel shall cooperate accordingly: 1. Pre-audit interview. 2. Onsite physical audit. The audited agency cannot give the explanations, collaborate or provide documentation for onsite inspector under the preceding paragraph for justifiable reasons under

辦理，並得停止稽核作業之全部或一部： 一、認有理由者，應將審核之依據及相關資訊記載於稽核結果報告。 二、認無理由者，應要求受稽核機關依第一項規定辦理；已停止稽核作業者，得擇期續行辦理，並於十日前以書面通知受稽核機關。	the law, they shall submit the reasons in writing to the competent authority. Upon receipt the preceding notice in writing, the competent authority shall verify it and then take the following actions, and may suspend all or part of the audit operations: 1. If the reasons are considered justifiable, it shall record the accordance and relevant information in the audit report. 2. If the reasons are considered groundless, it shall require the audited agency to follow the requirements of Paragraph 1; if the audit operations have been suspended, it may select other time periods to continue the audit and deliver the audit program notice in writing to the audited agency ten days before the audit.
第六條　主管機關辦理第三條第一項之稽核，應依同條第二項所定考量因素，就各受稽核機關分別組成三人以上之稽核小組。 主管機關組成前項稽核小組時，應考量稽核之需求，邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識之公務機關代表或專家學者擔任小組成員，其中公務機關代表不得少於全體成員人數之四分之一。 主管機關應以書面與稽核小組成員約定利益衝突之迴避及保密義務。 第二項之公務機關代表或專家學者，有下列情形之一者，應主動迴避擔任該次稽核之稽核小組成員： 三、本人、其配偶、三親等內親屬、家屬或上開人員財產信託之受託人，與受稽核機關或其負責人	Article 6　In conducting the audit under Paragraph 1 of Article 3, the competent authority shall form an audit team composed of three or more people respectively for each audited agency, depending on the considerations under Paragraph 2 of the same article. Informing the audit team under the preceding paragraph, the competent authority shall, taking the needs of the audit into consideration, invite representatives of government agencies or experts and scholars who have professional knowledge of cyber security policies or have professional knowledge of technologies, managements, law affairs required for such audit to act as members of such team, of which the number of representatives of the government agency may not be less than one-fourth of all members. The competent authority shall sign, in writing, with members of audit teams on recusal due to interest conflicts and confidentiality obligations. If the member of audit team under Paragraph 2 has any of the following circumstances, he shall

間有財產上或非財產上之利害關係。 四、本人、其配偶、三親等內親屬或家屬，與受稽核機關或其負責人間，目前或過去二年內有僱傭、承攬、委任、代理或其他類似之關係。 五、本人目前或過去二年內任職之機關（構）或單位，曾為受稽核機關之顧問，其輔導項目與受稽核項目相關。 六、其他情形足認擔任稽核小組成員，將對稽核結果之公正性造成影響。	avoid himself from acting as the member of that audit team: 1. He, his spouse, his relatives within the third degree, his family member, or the trustee of the property trusts of above-mentioned persons have a property or non-property interest relationship with the audited agency or the responsible person thereof. 2. He, his spouse, his relatives within the third degree or his family member has employment, contract, appointment, agency or other similar relationship with the audited agency or the responsible person in the current or the past two years. 3. He has served in the current or past two years to be a consultant of the audited agency and his mentoring project is related to the audit program. 4. Other circumstance that may be considered that his role as a member of the audit team might affect the impartiality of the audit result.
第七條　主管機關應於每季所定受稽核機關之稽核作業完成後一個月內，將稽核結果報告交付該季受稽核機關。 前項稽核結果報告之內容，應包括稽核之範圍、缺失或待改善事項、第五條第二項所定受稽核機關未能為說明、協力或提出資料供現場查閱之情形、理由與同條第三項所定主管機關審核結果，及其他與稽核相關之必要內容。	Article 7　The competent authority shall, within one month after the completion of the audit operations on the audited agency as designated for each quarter, deliver the audit reports to the audited agencies for the quarter. The contents of the preceding audit reports shall include the scope of the audit, flaws or items to be improved, the status and reasons for the failures of the audited agency to give explanations, collaborate or provide documentations for on-site inspections under Paragraph 2 of Article 5, and the audit results of the competent authority under Paragraph 3 of the same article, and other necessary contents relating to the audit.
第八條　受稽核機關經發現其資通安全維護計畫實施情形有缺失或待改善者，應於主管機關交付稽核結果報告後	Article 8　If flaws or items to be improved are found in the implementation of the cyber security maintenance plan, the audited agency shall submit

一個月內，依主管機關指定之方式提出改善報告，並送交中央目的事業主管機關；主管機關及中央目的事業主管機關認有必要時，得要求該受稽核機關進行說明或調整。 前項受稽核機關提出改善報告後，應依主管機關指定之方式及時間，提出改善報告之執行情形，並送交中央目的事業主管機關；主管機關認有必要時，得要求該受稽核機關進行說明或調整。	improvement report in the manner specified by the competent authority within one month after the competent authority has delivered the audit report, and shall deliver the same to the central authority in charge of the relevant industry. The competent authority and the central government authority in charge of the subject industry may require the audited agency to give explanations or make adjustments when necessary. After the improvement reports are submitted under the preceding paragraph, the audited agency shall submit the implementation status of the improvement reports in the manner and within the timeframe specified by the competent authority, and shall deliver the same to the central authority in charge of the relevant industry. The competent authority may require the audited agency to give explanations or make adjustments when necessary.
第九條　主管機關辦理第三條第一項之稽核，得要求受稽核機關之中央目的事業主管機關派員為必要協助。	Article 9　In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the central authority in charge of the relevant industry with the audited agency to dispatch personnel for necessary assistance.
第十條　本辦法之施行日期，由主管機關定之。 本辦法修正條文自發布日施行。	Article 10　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.

資通安全情資分享辦法-英譯對照

資通安全情資分享辦法	Cyber Security Information Sharing Regulations
第一條　本辦法依資通安全管理法（以下簡稱本法）第八條第二項規定訂定之。	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).
第二條　本辦法所稱資通安全情資（以下簡稱情資），指包括下列任一款內容之資訊： 十四、資通系統之惡意偵察或情蒐活動。 十五、資通系統之安全漏洞。 十六、使資通系統安全控制措施無效或利用安全漏洞之方法。 十七、與惡意程式相關之資訊。 十八、資通安全事件造成之實際損害或可能產生之負面影響。 十九、用以偵測、預防或因應前五款情形，或降低其損害之相關措施。 二十、其他與資通安全事件相關之技術性資訊。	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: 3. Malicious detections or collections activity of information and communication system. 4. Security vulnerabilities of information and communication system. 5. The methods that invalidate the information and communication systems security control measure or make use of the security vulnerability. 6. The information relating to malicious programs. 7. The actual damage or possible negative impact caused by cyber security incident. 8. Relevant measures that are taken to detect, prevent from or respond to the circumstances under the preceding five subparagraphs or to mitigate the damage. 9. Other technical information relating to cyber security incidents.
第三條　主管機關應就情資分享事宜進行國際合作。 主管機關應適時與公務機關進行情資分享。 公務機關應適時與主管機關	Article 3 The competent authority shall conduct international cooperation in the matters of cyber security information sharing. The competent authority shall timely

進行情資分享。但情資已依前項規定分享或已經公開者，不在此限。 中央目的事業主管機關應適時與其所管之特定非公務機關進行情資分享。 特定非公務機關得與中央目的事業主管機關進行情資分享。 前項分享之情資，經中央目的事業主管機關認定足以防止其他機關資通安全事件之發生或降低其損害者，中央目的事業主管機關得予以獎勵。	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.
第四條　情資有下列情形之一者，不得分享： 一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。 二、其他依法規規定應秘密或應限制、禁止公開之情形。 情資含有前項不得分享之內容者，得僅就其他部分分享之。	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.
第五條　公務機關或特定非公務機關（以下簡稱各機關）進行情資分享，應就情資進行分析及整合，並規劃適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。	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.
第六條　各機關應就所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。	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.
第七條　各機關進行情資整合時，得依情資之來源、接收日期、可用期間、類別、威脅指標特性及其他適當項目與內部情資進行關聯分析。 公務機關應就整合後發現之新型威脅情資進行分享。	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.
第八條　各機關應就所接收之情資，採取適當之安全維護措施，避免情	Article 8 For the cyber security information

資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。	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.
第九條 各機關進行情資分享，應分別依主管機關或中央目的事業主管機關指定之方式為之。 各機關因故無法依前項規定方式進行情資分享者，分別經主管機關或中央目的事業主管機關同意後，得以下列方式之一為之： 一、 書面。 二、 傳真。 三、 電子郵件。 四、 資訊系統。 五、 其他適當方式。	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.
第十條 未適用本法之個人、法人或團體，經主管機關或中央目的事業主管機關同意後，得與其進行情資分享。 主管機關或中央目的事業主管機關同意前項個人、法人或團體進行情資分享，應以書面與其約定應遵守第四條至前條之規定。	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.
第十一條 本辦法施行日期，由主管機關定之。 本辦法修正條文自發布日施行。	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.

資通安全情資分享辦法	Cyber Security Information Sharing Regulations
第一條　本辦法依資通安全管理法（以下簡稱本法）第八條第二項規定訂定之。	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).
第二條　本辦法所稱資通安全情資（以下簡稱情資），指包括下列任一款內容之資訊： 二十一、 資通系統之惡意偵察或情蒐活動。 二十二、 資通系統之安全漏洞。 二十三、 使資通系統安全控制措施無效或利用安全漏洞之方法。 二十四、 與惡意程式相關之資訊。 二十五、 資通安全事件造成之實際損害或可能產生之負面影響。 二十六、 用以偵測、預防或因應前五款情形，或降低其損害之相關措施。 二十七、 其他與資通安全事件相關之技術性資訊。	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: 10. Malicious detections or collections activity of information and communication system. 11. Security vulnerabilities of information and communication system. 12. The methods that invalidate the information and communication systems security control measure or make use of the security vulnerability. 13. The information relating to malicious programs. 14. The actual damage or possible negative impact caused by cyber security incident. 15. Relevant measures that are taken to detect, prevent from or respond to the circumstances under the preceding five subparagraphs or to mitigate the damage. 16. Other technical information relating to cyber security incidents.
第三條　主管機關應就情資分	Article 3 The competent authority shall conduct

享事宜進行國際合作。 主管機關應適時與公務機關進行情資分享。 公務機關應適時與主管機關進行情資分享。但情資已依前項規定分享或已經公開者，不在此限。 中央目的事業主管機關應適時與其所管之特定非公務機關進行情資分享。 特定非公務機關得與中央目的事業主管機關進行情資分享。	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.
第四條　情資有下列情形之一者，不得分享： 三、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。 四、其他依法規規定應秘密或應限制、禁止公開之情形。 情資含有前項不得分享之內容者，得僅就其他部分分享之。	Article 4 The cyber security information under any of the following circumstances may not be shared: 3. 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. 4. 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.
第五條　公務機關或特定非公務機關（以下簡稱各機關）進	Article 5 In conducting cyber security information sharing, the government agency or the specific

行情資分享，應就情資進行分析及整合，並規劃適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。	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.
第六條　各機關應就所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。	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.
第七條　各機關進行情資整合時，得依情資之來源、接收日期、可用期間、類別、威脅指標特性及其他適當項目與內部情資進行關聯分析。 公務機關應就整合後發現之新型威脅情資進行分享。	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.
第八條　各機關應就所接收之情資，採取適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。	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.
第九條 各機關進行情資分享，應分別依主管機關或中央目的事業主管機關指定之方式為之。 各機關因故無法依前項規定方式進行情資分享者，分別經主管機關或中央目的事業主管機關同意後，得以	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

下列方式之一為之： 六、 書面。 七、 傳真。 八、 電子郵件。 九、 資訊系統。 一〇、 其他適當方式。	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: 6. Written documents. 7. Fax. 8. Email. 9. Information system. 10. Other appropriate manner.
第十條 未適用本法之個人、法人或團體，經主管機關或中央目的事業主管機關同意後，得與其進行情資分享。 主管機關或中央目的事業主管機關同意前項個人、法人或團體進行情資分享，應以書面與其約定應遵守第四條至前條之規定。	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.
第十一條 本辦法施行日期，由主管機關定之。	Article 11 The date for enforcement of these Regulations shall be decided by the competent authority.