Cyber Security Management Act

2025-09-24

Hua-Zong-Yi-Yi No. 11400095391

CHAPTER I. GENERAL PROVISIONS

Article 1 This Cyber Security Management Act (hereinafter referred to as the Act) is duly stipulated in an effort to proactively carry out national cyber security policies and accelerate the construction of an environment for national cyber security, thereby safeguarding national security and protecting the public interests of all of society.

Article 2 The competent authority over the Act is the Ministry of Digital Affairs.

The execution of cyber security affairs shall be undertaken by a designated agency for cyber security as assigned by the Ministry of Digital Affairs.

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

1. Information and Communication Systems: refers to any system used for collecting, controlling, transmitting, storing, circulating, or deleting information, or for otherwise processing, using, or sharing information.
2. Information and Communication Services: refers to any services relating to the collection, control, transmission, storage, circulation, deletion, other processing, use, or sharing of information.
3. Cyber Security: refers to the prevention of unauthorized access to, use of, control over, disclosure of, damage to, alteration of, destruction of information or information and communication systems, or any other circumstances affecting the confidentiality, integrity, or availability of information or information and communication systems.
4. Cyber Security Incident: refers to any event where the status of a system, service, or network is identified as having a potential violation of the cyber security policy or a failure of protective measures, which affects the functionality of the information and communication system.
5. Government Agency: refers to a central, local government agency (organization), or public juristic person that exercises public power according to law, but excluding military and intelligence agencies.
6. Specific Non-Government Agency: refers to a critical infrastructure provider, a government-owned enterprise, a designated foundation, or any enterprise, organization, or institution under control of the government.
7. Critical Infrastructure: refers to physical or virtual assets, systems, or networks, the functions of which, once they cease to operate or their performance is reduced, may have a significant impact on national security, social and public interests, people's lives, or economic activities, and which are subject to periodic review and designation by the Executive Yuan.
8. Critical Infrastructure Provider: refers to any entity that maintains, operates or provides, in whole or

in part, critical infrastructure as designated by the the central competent authority in charge of the relevant sector, which shall be submitted to the Executive Yuan for approval.

9. Designated Foundation: refers to foundations that fall within the scope of Article 2, Paragraph 2 or 3, or Article 63, Paragraph 1 or 4 of the Foundations Act, and that qualify as nationwide foundations as defined in Article 2, Paragraph 8 of the same Act.
10. Enterprises, Organizations, or Institutions Controlled by Government: refers to enterprises, organizations, institutions publicly announced by the Ministry of Civil Service pursuant to Article 77, Paragraph 1, Subparagraph 2, Item 3 and 4 of the Public Service Pension, Severance and Compensation Act, that are of importance to cyber security, as designated by the central competent authority in charge of the relevant sector and approved by the competent authority; for those controlled by local governments, approval by the competent authority shall be granted only upon the consent of the relevant local competent authority.
11. Products Harmful to National Cyber Security: refers to information and communication systems, services, or products determined by the competent authority to pose a direct or indirect risk of harm to national cyber security, thereby affecting government operations or social stability.

Article 4 In an effort to promote cyber security, the government shall provide resources and integrate the strengths of the private sector and industries to boost the cyber security awareness of all people, and implement the following matters:

1. Cultivation of cyber security professionals.
2. Cyber security technology research and development, integration, application, and industry-academia cooperation, as well as international exchange and cooperation.
3. Development of the cyber security industry.
4. Development of cyber security-related software and hardware specifications, relevant services, and verification mechanisms.
5. Assist the private sector in handling, responding to, and preventing major cyber security incidents.

The promotion of the matters provided in the preceding paragraph shall be carried out by the competent authority through the formulation of the National Cyber Security Development Program, which shall be implemented upon approval by the Executive Yuan.

Article 5 For the purpose of implementing national cyber security policies, government agencies at all levels, both central and local, shall endeavor to cooperate in promoting and executing cyber security measures, jointly building a secure national cyber security environment.

To provide consultation and deliberation on national cyber security policies, response mechanisms, and major projects, and to coordinate cyber security-related affairs among central and local government agencies, the Executive Yuan shall convene, on a regular basis, the National Information and Communication Security Taskforce, to be chaired by the Premier or Vice Premier of the Executive

Yuan. Experts, scholars, and representatives of private organizations may be invited to attend; extraordinary meetings may also be convened when necessary. Secretariat affairs of the Taskforce shall be handled by the competent authority.

Resolutions adopted by the National Information and Communication Security Taskforce meetings as provided in the preceding paragraph shall be implemented by the relevant government agencies. The competent authority shall conduct regular follow-up reviews, performance monitoring, and, where appropriate, performance evaluations.

The rules governing the composition, functions, procedures, and other related matters of the National Information and Communication Security Taskforce under Paragraph 2 shall be prescribed by the Executive Yuan.

Article 6 The competent authority shall plan and promote national cyber security policies, the development of cyber security technologies, international exchanges and cooperation, and overall cyber security protection measures, as well as publish annually a National Cyber Security Status Report, an Audit Summary Report on the implementation of cyber security maintenance plans, and a National Cyber Security Development Program.

The reports and program provided in the preceding paragraph shall be submitted by the competent authority to the Legislative Yuan for recordation.

Article 7 Government agencies and specific non-government agencies shall, based on the importance and sensitivity of their operations, their hierarchical levels, the type, volume, and nature of the information they hold or process, and the scale and nature of their information and communication systems, report to the competent authority for approval or recordation of their respective cyber security responsibility levels.

Government agencies and specific non-government agencies shall comply with the requirements of their cyber security responsibility levels, and shall implement cyber security protection measures from the perspectives of management, technology, awareness, and training.

The criteria for distinguishing cyber security responsibility levels referred to in the preceding two paragraphs, the procedures for approval or recordation, applications for changes, the items and contents of cyber security protection measures, the qualifications and allocations of dedicated personnel, and other related matters shall be prescribed by the competent authority.

Article 8 The competent authority may conduct periodic or ad hoc audits of the implementation of cyber security maintenance plans by government agencies and specific non-government agencies.

Where deficiencies or areas for improvement are identified in the audit provided in the preceding paragraph, the audited agency shall submit a corrective action report. Government agencies shall submit such reports to the authority designated under Article 14 to receive implementation reports; specific

non-government agencies shall submit such reports to the central competent authority in charge of the relevant sector, which shall forward them to the competent authority after review.

The authority receiving the corrective action report, as provided in the preceding paragraph, may, where deemed necessary, require the audited agency to provide explanations or make adjustments.

The frequency, scope, and methods of audits of the implementation of cyber security maintenance plans, as provided in the preceding three paragraphs, the submission of corrective action reports, and other related matters shall be prescribed by the competent authority.

Audits under Paragraph 1 shall be carried out pursuant to an annual plan prepared by the competent authority and approved by the Executive Yuan. The annual plan and the annual results report shall be submitted to the National Information and Communication Security Taskforce for recordation.

Article 9 The competent authority shall set up a mechanism for sharing cyber security intelligence.

The analysis and integration of cyber security intelligence provided in the preceding paragraph, the rules of sharing contents, procedures, methods, and other related matters shall be prescribed by the competent authority.

Article 10 Government agencies or specific non-government agencies, within the scope of this Act, that outsource the implementation, maintenance and operation of information and communication systems or the provision of information and communication services shall select appropriate contractors, require the contractors to establish effective cyber security management mechanisms, and supervise the implementation of such mechanisms.

The procedures and environments in which contractors referred to in the preceding paragraph perform outsourced tasks shall incorporate comprehensive cyber security management measures or obtain impartial third-party certification.

Government agencies or specific non-government agencies that handle outsourced tasks as described in Paragraph 1 shall enter into a written agreement with the contractor, specifying the rights and obligations of both parties as well as liabilities for breaches.

Government agencies or specific non-government agencies shall cooperate with the competent authority in planning and conducting cyber security drills and, if necessary, incorporate third-party assistance mechanisms. The contents of such drills and other relevant matters shall be prescribed by the competent authority.

Chapter II Government Agency Cyber Security Management

Article 11 Government agencies shall not download, install, or use products are harmful to national cyber security. The same shall apply to any broadcasting equipment or Internet access services provided to the public at

facilities operated directly or outsourced by the government agency, when necessary to maintain cyber security. However, if such use is required for official duties with no alternative solutions, the agency may, with approval from its Chief Information Security Officer and the Chief Information Security Officer of the agency responsible for receiving implementation reports under Article 14, submit a written request to the competent authority for approval to use the product on a case-by-case basis, with proper record-keeping.

Products are harmful to national cyber security shall not be downloaded, installed, or used on information and communication equipment distributed by government agencies for official use, and must comply with relevant laws and regulations. However, if such use is required for official duties with no alternative solutions, the provisions of the preceding paragraph shall apply mutatis mutandis.

The review procedures, risk assessments, information sharing, usage restrictions, and other related matters regarding products are harmful to national cyber security, as provided in the preceding two paragraphs, shall be formulated by the competent authority in consultation with relevant agencies and submitted to the Executive Yuan for approval.

Article 12 Government agencies shall establish the position of Chief Information Security Officer, to be concurrently held by the deputy head or other appropriate personnel designated by the head of the agency. The Chief Information Security Officer shall be responsible for promoting and overseeing the agency's cyber security-related affairs.

Article 13 Government agencies shall comply with the requirements corresponding to their assigned cyber security responsibility levels and, considering the type, volume, and nature of the information they possess or process, as well as the scale and nature of their information and communication systems, shall formulate, revise, and implement cyber security maintenance plans.

Article 14 Government agencies shall annually submit reports on the implementation of their cyber security maintenance plans to their superior or supervisory authorities. Agencies without superior or supervisory authorities shall handle the submission of their cyber security maintenance plan reports in accordance with the following provisions:

1. The Office of the President, the National Security Council, and the Five Yuans shall submit to the competent authority.
2. Municipal governments, municipal councils, county (city) governments, and county (city) councils shall submit to the competent authority.
3. District offices of indigenous districts in special municipalities and their representative councils shall submit to the municipal government; township (town, city) offices and their representative councils shall submit to the county government.

Article 15 Government agencies shall audit the implementation of cyber security maintenance plans by their

subordinate and supervised agencies, township (town, city) offices under their jurisdiction, district offices of indigenous districts in special municipalities, and representative councils of townships (towns, cities) as well as indigenous districts in special municipalities.

Article 16 Where deficiencies or areas for improvement are identified in the implementation of the cyber security maintenance plan of an audited agency, the audited agency shall submit a corrective action report to the auditing agency, which shall, in turn, submit the said report together with the audit results to the competent authority in the manner prescribed.

Where deemed necessary, the auditing agency or the competent authority may require the audited agency to provide explanations or make adjustments.

The matters relating to the essential elements of the cyber security maintenance plan provided in the preceding three Articles and in Paragraph 1, the submission of implementation status reports, the frequency, contents, and methods of audits, the delivery of results, the submission of corrective action reports, and other related matters shall be prescribed by the competent authority.

Article 17 Government agencies shall establish a reporting and response mechanism to address cyber security incidents.

When government agencies become aware of a cyber security incident, they shall report such an incident to both the agency designated under Article 14 to receive its implementation status report and the competent authority.

The government agency shall submit, to the notified agency provided in the preceding paragraph, an investigation, handling, and corrective action report regarding the cyber security incident.

The rules regarding the necessary items of the reporting and response mechanisms provided in the preceding three paragraphs, the reporting content, the submission of reports, the conduct of drills, and other related matters shall be prescribed by the competent authority.

Where the agency notified under Paragraph 2 becomes aware of a major cyber security incident, it may provide relevant assistance to the government agency concerned, and, when appropriate, may announce the necessary information and corresponding countermeasures relating to the incident.

Article 18 Government agencies shall, in compliance with the requirements of their assigned cyber security responsibility levels, appoint dedicated cyber security personnel to handle cyber security affairs and incident responses. Personnel with proven performance in their cyber security duties shall be commended.

The competent authority shall properly plan and promote the professional training of dedicated cyber security personnel to enhance their expertise in cyber security. In the event of a major cyber security incident, the competent authority may mobilize cyber security personnel from agencies at all levels to provide support.

The rules governing the commendation, professional training, mobilization, performance evaluation, and other related matters of the personnel provided in the preceding two paragraphs shall be prescribed by the competent authority.

Article 19 Government agencies may, when necessary, conduct suitability reviews of their dedicated cyber security personnel.

The competent authority may, after the announcement of the results of the cyber security personnel recruitment examination, conduct suitability reviews of the successful candidates.

Personnel who refuse to undergo such reviews, or who fail to pass the reviews conducted pursuant to the preceding two paragraphs as determined by the employing agency, shall not engage in cyber security affairs involving national secrets, military secrets, or national defense secrets.

The positions of such personnel may be adjusted by the employing agency in accordance with law, based on internal management considerations and operational needs.

The records of reviews conducted under Paragraphs 1 and 2 shall be handled in confidence by the employing agency in accordance with applicable regulations and shall be properly preserved, and shall not be used for any other purposes. Violations shall be subject to disciplinary action depending on the severity of the circumstances.

The rules governing the authorities responsible for conducting reviews, the personnel subject to review, the review procedures, contents, and other related matters shall be prescribed by the competent authority in consultation with the relevant authorities.

Chapter III. Specific Non-Government Agency Cyber Security Management

Article 20 The central competent authority in charge of the relevant sector shall, after consulting relevant government agencies, private organizations, and experts and scholars, designate critical infrastructure providers, submit the designation to the competent authority for approval by the Executive Yuan, and notify the approved entities in writing.

Critical infrastructure providers shall comply with the requirements of their assigned cyber security responsibility levels, appoint dedicated cyber security personnel, and considering the types, volume, and nature of the information they possess or process, as well as the scale and nature of the information and communication systems, formulate, revise, and implement cyber security maintenance plans.

Critical infrastructure providers shall report on the implementation of their cyber security maintenance plans to the central competent authority in charge of the relevant sector.

The central competent authority in charge of the relevant sector shall, taking into comprehensive consideration the importance and sensitivity of the business of the critical infrastructure providers under

its supervision, the scale and nature of the information and communication systems, the frequency and severity of cyber security incidents, and other cyber security-related factors, conduct periodic audits of the implementation of their cyber security maintenance plans.

Where deficiencies or areas for improvement are identified in the implementation of a critical infrastructure provider's cyber security maintenance plan, the provider shall submit a corrective action report to the central competent authority in charge of the relevant sector.

The central competent authority in charge of the relevant sector shall, in the manner prescribed, submit the audit results and corrective action reports to the competent authority.

Article 21 Specific non-government agencies other than critical infrastructure providers shall comply with the requirements of their assigned cyber security responsibility levels, appoint dedicated cyber security personnel, and, considering the types, volume, and nature of the information they possess or process, as well as the scale and nature of their information and communication systems, formulate, revise, and implement cyber security maintenance plans.

The central competent authority in charge of the relevant sector may require the specific non-government agencies under its supervision provided in the preceding paragraph to report on the implementation of their cyber security maintenance plans.

The central competent authority in charge of the relevant sector may audit the implementation of the cyber security maintenance plans of the specific non-government agencies under its supervision provided in Paragraph 1. Where deficiencies or areas for improvement are identified, the audited specific non-government agencies shall, within a designated period, submit corrective action report.

The central competent authority in charge of the relevant sector shall, in the manner prescribed, submit the audit results and corrective action reports to the competent authority.

Article 22 The matters relating to the essential elements of the cyber security maintenance plans provided in the preceding two articles, the submission of implementation status reports, the frequency, contents, and methods of audits, the delivery of results, the submission of corrective action reports, and other matters to be followed shall be formulated by the central competent authority in charge of the relevant sector and submitted to the competent authority for approval.

Article 23 Specific non-government agencies shall appoint a Chief Information Security Officer, who shall be a representative, manager, other person with authority, or an appropriate designated member of personnel, responsible for promoting and overseeing the specific non-government agency's cyber security-related affairs.

Article 24 Specific non-government agencies shall establish notification and response mechanisms for cyber security incidents.

When specific non-government agencies become aware of a cyber security incident, they shall notify the central competent authority in charge of the relevant sector of the incident.

The specific non-government agency shall submit an investigation, handling, and corrective action report regarding the cyber security incident to the central competent authority in charge of the relevant sector; in the case of a major cyber security incident, the report shall also be submitted to the competent authority.

The rules regarding the necessary items of the reporting and response mechanism, the reporting content, submission of reports, delivery, drill exercises, and other matters to be followed provided in the preceding three paragraphs shall be prescribed by the competent authority.

When the central competent authority in charge of the relevant sector or the competent authority becomes aware of a major cyber security incident, it shall provide necessary assistance; at an appropriate time, it may also announce the necessary information and response measures relating to the incident.

Article 25 The central competent authority in charge of the relevant sector, for the purpose of investigating a major cyber security incident occurring at a specific non-government agency, may carry out the investigation in accordance with the following procedures:

1. Notify the parties concerned or related parties to provide statements in person.
2. Notify the parties concerned and related parties to submit forensic or investigative reports issued by independent third-party institutions.
3. Dispatch personnel, appoint or commission other agencies (organizations) to conduct necessary inspections at the premises of the parties concerned and related parties.

The related parties provided in the preceding paragraph are limited to contractors entrusted by the specific non-government agency to establish, maintain, operate or provide information and communication systems or information and communication services that are related to the major cyber security incident.

The parties concerned or related parties shall not evade, obstruct, or refuse any investigation conducted by the central competent authority in charge of the relevant sector pursuant to Paragraph 1.

Personnel carrying out the investigation shall present identification or proof of authority for performing their duties; if such identification or proof is not presented, investigated parties may refuse compliance.

Agencies (organizations) appointed or commissioned under Paragraph 1, Subparagraph 3 shall not disclose any confidential information of the specific non-government agency acquired while performing their assigned or commissioned duties.

Article 26 Personnel of specific non-government agencies with proven performance in their cyber security duties

shall be commended.

Article 27 The central competent authority in charge of the relevant sector may restrict or prohibit a specific non-government agency from downloading, installing, or using products are harmful to national cyber security. The same shall apply to any broadcasting equipment or Internet access services provided to the public at facilities operated directly or outsourced by the specific non-government agency, when necessary to maintain cyber security. However, if such use is required for official duties with no alternative solutions, the specific non-government agency may, with approval from the Chief Information Security Officer of the agency, submit a written report to the central competent authority in charge of the relevant sector for approval to use the product on a case-by-case basis, with proper record-keeping.

The control measures restricting or prohibiting the use of products are harmful to national cyber security by specific non-government agencies, as provided in the preceding paragraph, shall be prescribed by the central competent authority in charge of the relevant sector and submitted to the competent authority for recordation.

Chapter IV. Penalties

Article 28 Personnel of government agencies who fail to perform duties in accordance with the provisions of this Act shall be subject to disciplinary sanctions or disciplinary actions in accordance with relevant regulations, depending on the severity of the case.

The rules for the disciplinary actions provided in the preceding paragraph shall be prescribed by the competent authority.

Personnel of specific non-government agencies who fail to perform duties in accordance with the provisions of this Act, and where the circumstances are significant, shall be subject to disciplinary action by the specific non-government agency in accordance with relevant regulations.

Article 29 If specific non-government agencies fail to report a cyber security incident in accordance with Paragraph 2, Article 24, the central competent authority in charge of the relevant sector shall impose a fine of not less than NT$300,000 and not more than NT$10,000,000 and shall order correction within a specified period; if correction is not made within the prescribed period, additional fines shall be imposed for each violation.

Article 30 Where specific non-government agencies fall under any of the following circumstances, the central competent authority in charge of the relevant sector shall order correction within a specified period; if correction is not made within the prescribed period, a fine of not less than NT$100,000 and not more than NT$5,000,000 shall be imposed for each violation:

1. Failure to formulate, revise, or implement a cyber security maintenance plan in accordance with Paragraph 2, Article 20 or Paragraph 1, Article 21, or violation of the requirement regarding essential

elements of the cyber security maintenance plan as provided in the measures prescribed under Article 22.

2. Failure to submit the implementation status of the cyber security maintenance plan to the central competent authority in charge of the relevant sector in accordance with Paragraph 3, Article 20,or Paragraph 2, Article 21, or violation of the provisions on the submission of implementation status reports as prescribed under Article 22.
3. Failure to submit a corrective action report to the central competent authority in charge of the relevant sector in accordance with Paragraph 2, Article 8, Paragraph 5, Article 20, or Paragraph 3, Article 21, or violation of the provisions on the submission of corrective action reports as prescribed under Article 22.
4. Failure to formulate a notification and response mechanism for cyber security incidents in accordance with Paragraph 1, Article 24, or violation of the requirements regarding the essential elements of the reporting and response mechanism as prescribed under Paragraph 4, Article 24.
5. Failure to submit investigation, handling, and corrective action reports of cyber security incidents to the central competent authority in charge of the relevant sector, or to the competent authority in accordance with Paragraph 3, Article 24, or violation of the provisions on the submission and delivery of such reports as prescribed under Paragraph 4, Article 24.
6. Violation of the provisions regarding the contents of notifications and the execution of drills as prescribed under Paragraph 4, Article 24.

Article 31 Those who evade, obstruct, or refuse an investigation in violation of Paragraph 3, Article 25 shall be subject to a fine of not less than NT$100,000 and not more than NT$1,000,000 imposed by the central competent authority in charge of the relevant sector.

Chapter V. Supplementary Provisions

Article 32 The competent authority may entrust other government agencies, juristic persons, or organizations to handle matters related to overall cyber security protection, drills, audits, international exchange and cooperation, and other cyber security-related affairs.

The entrusted government agencies, juristic persons, or organizations provided in the preceding paragraph shall not disclose any confidential information they become aware of in the course of handling the entrusted matters.

Where the business of a specific non-government agency falls under the jurisdiction of multiple central competent authorities in charge of the relevant sector, the competent authority may coordinate and designate one or more of such central competent authorities in charge of the relevant sector to handle, individually or jointly, the matters that shall be carried out by the central competent authority in charge of the relevant sector provided in this Act.

Article 33 In the event that a cyber security incident defined under this Act involves the personal data breach, government agencies and specific non-government agencies shall handle the matter separately in accordance with the Personal Data Protection Act and its related laws and regulations.

Article 34 The enforcement rules of this Act shall be stipulated by the competent authority.

Article 35 The implementation date of this Act shall be stipulated by the Executive Yuan.