Regulations on the Security Protection of Critical Information Infrastructure

Dan Young Business Consultancy — www.danyoungcpa.com

Unofficial English translation prepared for reference only. The official Chinese text prevails.

Adopted at the 133rd Executive Meeting of the State Council on April 27, 2021; promulgated by Decree No. 745 of the State Council of the People's Republic of China on July 30, 2021
Effective: September 1, 2021

Article 1 — These Regulations are formulated in accordance with the Cybersecurity Law of the People's Republic of China for the purpose of ensuring the security of critical information infrastructure and maintaining cybersecurity.

Article 2 — These Regulations shall apply to the security protection of critical information infrastructure within the territory of the People's Republic of China.

Article 3 — Critical information infrastructure refers to important network facilities and information systems in important industries and fields such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, and national defense science, technology and industry, as well as other important network facilities and information systems that, if destroyed, functionally impaired, or subject to data leakage, may seriously endanger national security, the national economy and people's livelihood, or the public interest.

Article 4 — The protection of critical information infrastructure shall adhere to the principles of comprehensive coordination, division of responsibilities, and protection in accordance with law, and shall implement a working mechanism under which the cybersecurity department coordinates, functional departments supervise, and operators take primary responsibility.

Article 5 — The state cybersecurity department shall be responsible for overall coordination of the security protection of critical information infrastructure, and for organizing the formulation of rules for the designation of critical information infrastructure.

The relevant departments in charge of the protection of critical information infrastructure under the State Council shall organize the designation of critical information infrastructure in their respective industries and fields, supervise and guide the security protection of critical information infrastructure in their respective industries and fields, and formulate rules for the designation of critical information infrastructure in their respective industries and fields.

The relevant departments of the State Council such as public security, state security, state secrecy administration, cryptography administration, and telecommunications shall, within their respective scope of duties, be responsible for the security protection of critical information infrastructure.

Article 6 — An operator of critical information infrastructure shall bear primary responsibility for the security protection of the critical information infrastructure under its operation, perform the obligations of cybersecurity protection, accept the supervision and management of the government and the public, and bear social responsibilities.

Article 7 — Important industries and fields, such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, and national defense science, technology and industry, shall be important industries and fields for the protection of critical information infrastructure. The departments in charge of the protection of critical information infrastructure shall, in light

Source: https://www.danyoungcpa.com/critical-information-infrastructure-security-protection-regulations-prc-2021-english-translation/

of the actual circumstances of their respective industries and fields, formulate rules for the designation of critical information infrastructure and report them to the state cybersecurity department for filing.

Article 8 — The key factors for the designation of critical information infrastructure include:

(1) The degree of criticality of network facilities, information systems, and so on to the core businesses of the industry or field;

(2) The degree of harm that may be caused if network facilities, information systems, and so on are destroyed, functionally impaired, or subject to data leakage;

(3) The associated impact on other industries and fields.

Article 9 — The departments in charge of the protection of critical information infrastructure shall, in accordance with the designation rules, organize the designation of critical information infrastructure in their respective industries and fields and promptly notify the operators of the designation results.

Article 10 — The designated critical information infrastructure shall undergo a review by the departments in charge of the protection of critical information infrastructure. If any major changes occur or if the review identifies a need for re-designation, the operator shall promptly report to the department in charge.

Article 11 — Operators of critical information infrastructure shall set up a special security management body to be responsible for the security protection of critical information infrastructure, and implement the security protection measures in accordance with these Regulations and other relevant provisions.

Article 12 — The special security management body of an operator of critical information infrastructure shall perform the following duties:

(1) Establish and improve rules and regulations on cybersecurity management;

(2) Organize the formulation of cybersecurity plans;

(3) Conduct cybersecurity monitoring and risk assessment;

(4) Formulate emergency response plans for cybersecurity incidents and conduct regular emergency drills;

(5) Report cybersecurity incidents or major cybersecurity risks in a timely manner in accordance with relevant provisions;

(6) Organize cybersecurity education and training;

(7) Perform other duties provided by laws and regulations.

Article 13 — The person in charge of the special security management body of an operator of critical information infrastructure shall be a member of the operator's leadership and shall have the professional knowledge and management experience appropriate to the security protection work of critical information infrastructure.

Article 14 — Operators of critical information infrastructure shall ensure that the special security management body has adequate staffing and financial resources commensurate with the scale of the critical information infrastructure and the security protection work.

Article 15 — Operators of critical information infrastructure shall conclude security and confidentiality agreements with employees in key cybersecurity positions, specifying the rights and obligations for cybersecurity and confidentiality.

Article 16 — Operators of critical information infrastructure shall give priority to procuring secure and reliable network products and services. Where network products and services may affect national security, they shall pass a security review organized by the state cybersecurity department in conjunction with relevant departments of the State Council in accordance with the provisions of the state.

Source: https://www.danyoungcpa.com/critical-information-infrastructure-security-protection-regulations-prc-2021-english-translation/

Article 17 — Operators of critical information infrastructure shall conduct cybersecurity testing and risk assessment at least once a year, either by themselves or by entrusting a cybersecurity service institution, and shall promptly rectify discovered security problems and report the testing and assessment results, as well as the rectification measures, to the relevant department in charge of the protection of critical information infrastructure.

Article 18 — Where an operator of critical information infrastructure procures network products and services, it shall sign a security and confidentiality agreement with the provider in accordance with the provisions of the state, specifying the obligations of the provider in technical support, security and confidentiality, and so on, and supervise the provider's performance of these obligations.

Article 19 — Operators of critical information infrastructure shall, in accordance with the provisions of the state, conduct background checks on the providers of network products and services that they intend to procure. They shall not procure network products and services from providers that fail to pass the security review or that have engaged in conduct endangering national security.

Article 20 — Where an operator of critical information infrastructure merges, demerges, or dissolves, it shall promptly report to the relevant department in charge of the protection of critical information infrastructure and handle the security protection of the critical information infrastructure in accordance with the requirements of the department in charge.

Article 21 — Operators of critical information infrastructure shall give priority to procuring secure and reliable network products and services. Network products and services that may affect national security shall pass a security review.

The relevant departments in charge of the protection of critical information infrastructure shall formulate standards and guidelines for the security procurement of network products and services for critical information infrastructure and strengthen supervision and management.

Article 22 — The department in charge of the protection of critical information infrastructure shall, within its scope of duties, supervise the security protection work of operators of critical information infrastructure, and may take the following measures:

(1) Conduct on-site inspections of the implementation of the security protection of critical information infrastructure;

(2) Conduct remote testing of the security risks of critical information infrastructure;

(3) Require the operator to provide relevant documents, records, and data;

(4) Entrust a specialized institution to conduct a technical inspection.

Article 23 — The department in charge of the protection of critical information infrastructure shall keep confidential the state secrets, trade secrets, and personal information obtained in the performance of its duties and shall not disclose, sell, or illegally provide such information to others.

Article 24 — Where the department in charge of the protection of critical information infrastructure discovers, during supervision and inspection, any security problems with the critical information infrastructure, it shall propose rectification suggestions and order the operator to rectify within a specified time limit. If the operator fails to rectify within the specified time limit, the department in charge may interview the operator's responsible person.

Article 25 — The state cybersecurity department shall establish a special work mechanism for the security protection of critical information infrastructure, organize specialized forces to provide technical support, and uniformly regulate information sharing, monitoring and early warning, emergency response, and other work related to network security.

Source: https://www.danyoungcpa.com/critical-information-infrastructure-security-protection-regulations-prc-2021-english-translation/

Article 26 — The state cybersecurity department shall establish a cybersecurity information sharing mechanism to promptly collect, assess, and share cybersecurity threat information and cybersecurity incident information.

Article 27 — The departments in charge of the protection of critical information infrastructure shall establish and improve the cybersecurity monitoring, early warning, and information notification systems in their respective industries and fields, and guide operators of critical information infrastructure in taking security protection measures.

Article 28 — Where an operator of critical information infrastructure discovers a major cybersecurity incident or a major cybersecurity threat, it shall report to the relevant department in charge of the protection of critical information infrastructure and the relevant public security organ in accordance with the provisions.

Article 29 — The state cybersecurity department shall, in conjunction with relevant departments, establish a cybersecurity emergency response mechanism for critical information infrastructure and formulate emergency response plans. The departments in charge of the protection of critical information infrastructure shall regularly organize emergency drills for cybersecurity in their respective industries and fields.

Article 30 — Operators of critical information infrastructure shall formulate emergency response plans for cybersecurity incidents and conduct regular emergency drills. In the event of a cybersecurity incident, the operator shall initiate the emergency response plan, take appropriate remedial measures, and report to the relevant authorities in accordance with the provisions.

Article 31 — The state shall implement key protection of critical information infrastructure. No organization or individual may illegally invade, interfere with, or damage critical information infrastructure, and may not endanger the security of critical information infrastructure.

Article 32 — The state shall prioritize the use of secure and reliable network products and services that meet the relevant state standards for critical information infrastructure and encourage priority procurement of such products and services by operators of critical information infrastructure.

Article 33 — The state shall adopt measures to encourage specialized institutions to engage in the work of testing, assessment, and certification of the security of critical information infrastructure, and shall encourage and support innovation in science and technology and industrial development in relation to the security of critical information infrastructure.

Article 34 — Where an operator of critical information infrastructure fails to perform its obligations of security protection of critical information infrastructure in accordance with these Regulations, the relevant department in charge shall impose penalties in accordance with the Cybersecurity Law of the People's Republic of China and other relevant laws and administrative regulations.

Article 35 — These Regulations shall enter into force on September 1, 2021.

Disclaimer: This English translation is provided for informational and reference purposes only. It is not an official translation and has no legal effect. While we strive for accuracy, this translation may contain errors or omissions. For any legal matters or official purposes, please consult the original Chinese text or seek professional legal advice. Dan Young Business Consultancy assumes no liability for any reliance placed on this translation.

Source: https://www.danyoungcpa.com/critical-information-infrastructure-security-protection-regulations-prc-2021-english-translation/