Measures for 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.

Contents

Table of Contents 1

Chapter I — General Provisions 1

Chapter II — Designation of Critical Information Infrastructure 2

Chapter III — Obligations of CII Operators 2

Chapter IV — Safeguard and Promotion 3

Chapter V — Legal Liability 4

Chapter VI — Supplementary Provisions 4

Adopted at the 29th 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

Table of Contents

- Chapter I — General Provisions
- Chapter II — Designation of Critical Information Infrastructure
- Chapter III — Obligations of CII Operators
- Chapter IV — Safeguard and Promotion
- Chapter V — Legal Liability
- Chapter VI — Supplementary Provisions

Chapter I — General Provisions

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

Article 2 — The term "critical information infrastructure" (CII) as used in these Regulations means important network facilities and information systems in key industries and sectors, such as public communication and information services, energy, transport, water conservancy, finance, public services, e-government, and science and technology for national defense, as well as other important network facilities and information systems that, if damaged, incapacitated or subject to data leakage, may seriously endanger national security, the national economy, the people's livelihood or the public interest.

Source: https://www.danyoungcpa.com/critical-information-infrastructure-security-protection-measures-2021/

Article 3 — CII security protection shall adhere to the principles of comprehensive coordination, division of responsibilities, and protection according to law, and shall implement a protection system under which the principal responsibility lies with the CII operator, with government oversight, and broad participation by all sectors of society.

Article 4 — The national cyberspace administration authority shall be responsible for the overall planning and coordination of CII security protection. The public security department and the national security department under the State Council shall, within their respective scopes of functions and duties, be responsible for CII security protection. The competent departments of key industries and sectors under the State Council shall be responsible for the supervision and administration of CII security protection in their respective industries and sectors. The relevant departments of the people's governments at or above the provincial level shall, in accordance with their respective functions and duties, be responsible for CII security protection.

Chapter II — Designation of Critical Information Infrastructure

Article 5 — The competent departments of key industries and sectors (hereinafter referred to as "protection work departments") shall formulate CII designation rules for their respective industries and sectors based on the characteristics of the industry and sector and the actual needs of CII security protection, and report the rules to the public security department under the State Council for record.

Article 6 — The protection work departments shall, in accordance with the CII designation rules, organize the designation of CII in their respective industries and sectors and notify the CII operators of the designation results in writing. In the course of designation, the importance of network facilities and information systems to the key core businesses of the industry or sector, and the degree of harm that may result from damage, incapacitation or data leakage of the network facilities and information systems, shall be fully taken into consideration. The protection work departments shall report the designation results to the public security department under the State Council.

Article 7 — Where major changes occur in CII, rendering it unable to meet the designation criteria, the CII operator shall promptly report the matter to the protection work department. The protection work department shall, within three months, complete the re-examination and make a decision as to whether to remove the designation, and notify the CII operator of the decision in writing. The protection work department shall report the removal of designation to the public security department under the State Council.

Article 8 — Where CII operators disagree with the designation results, they may, within 15 working days of receiving the written notice, submit their opinions and supporting materials to the protection work department. The protection work department shall, within 30 working days of receiving the opinions, make a decision and notify the CII operator in writing.

Chapter III — Obligations of CII Operators

Article 9 — CII operators shall establish and improve their cybersecurity protection systems and responsibility systems, and ensure the security of CII in terms of organization, personnel, financial resources and technical measures.

Article 10 — CII operators shall designate a dedicated security management body and assign full-time security management personnel. The security management body shall perform the following duties:

(1) Establish and improve rules and regulations for network security management, and formulate emergency response plans and conduct drills;

(2) Conduct regular network security education, technical training and skill assessments for employees;

(3) Perform security monitoring, risk assessment and early warning of CII;

(4) Perform daily maintenance and management of CII security protection facilities;

Source: https://www.danyoungcpa.com/critical-information-infrastructure-security-protection-measures-2021/

(5) Formulate emergency response plans and conduct regular drills;

(6) Carry out security incident reporting and emergency response;

(7) Fulfill other duties as prescribed by laws and administrative regulations.

Article 11 — CII operators shall conduct cybersecurity inspections and risk assessments of CII at least once a year, either by themselves or by commissioning specialized cybersecurity service institutions, to promptly identify potential security risks and take remedial measures.

Article 12 — CII operators shall, when purchasing network products and services, conduct security review in accordance with the relevant provisions of the State. Where network products and services may affect national security, a security review shall be submitted to the national cyberspace administration authority, in conjunction with the relevant departments under the State Council, in accordance with the measures for security review of network products and services as prescribed by the State.

Article 13 — CII operators shall sign security and confidentiality agreements with providers of network products and services, specifying the obligations and responsibilities of the providers in respect of technical support, security and confidentiality, and other matters.

Article 14 — Personal information and important data collected and generated by CII operators during their operations within the territory of China shall be stored within the territory of China. Where it is necessary to provide such data abroad due to business requirements, a security assessment shall be conducted in accordance with the measures for security assessment of cross-border data transfer as formulated by the national cyberspace administration authority in conjunction with the relevant departments under the State Council. Where laws, administrative regulations or the relevant provisions of the State provide otherwise, those provisions shall prevail.

Article 15 — Where a merger, division, dissolution or other major change occurs in a CII operator, the CII operator shall report the matter to the protection work department and handle the CII in accordance with the requirements of the protection work department to ensure its security.

Article 16 — CII operators shall conduct background checks on the persons in charge of the security management body and key positions, and the public security department and the national security department shall provide assistance.

Article 17 — CII operators shall establish and implement a security reporting system. Where a major cybersecurity incident occurs in CII or a major cybersecurity threat is discovered, the operator shall report to the protection work department and the public security department in accordance with the relevant provisions.

Chapter IV — Safeguard and Promotion

Article 18 — Protection work departments shall establish and improve CII security monitoring, early warning and information sharing mechanisms, and promptly grasp the CII security situation, security risks and security incidents in their respective industries and sectors.

Article 19 — The national cyberspace administration authority shall, in conjunction with the public security department, the national security department and other relevant departments under the State Council, establish a CII security information sharing mechanism to promptly compile, verify, share and release CII security threats, vulnerabilities, incidents and other such information.

Article 20 — The national cyberspace administration authority shall, in conjunction with the public security department, the national security department and other relevant departments under the State Council, organize CII security inspections to identify security risks and propose improvement measures. CII operators shall cooperate with such inspections.

Article 21 — The State shall encourage and support research and development in CII security technologies and promote the application of CII security technologies. The State shall encourage CII operators to prioritize the procurement of secure and trustworthy network products and services.

Article 22 — The State shall support the training of specialized personnel in CII security and carry out CII security publicity, education and training.

Article 23 — No organization or individual shall carry out activities that illegally invade, interfere with or damage CII, or endanger the security of CII. No organization or individual shall provide programs or tools specifically used for invading, interfering with or damaging CII. Where the provision of programs or tools for purposes of cybersecurity protection or research is necessary, advance approval shall be obtained from the relevant State department.

Chapter V — Legal Liability

Article 24 — Where a CII operator fails to perform its CII security protection obligations in accordance with these Regulations, the relevant competent department shall, in accordance with its functions and duties, order the operator to take corrective action and issue a warning. Where the circumstances are serious, a fine of not less than RMB 100,000 but not more than RMB 1,000,000 shall be imposed, and the persons directly in charge shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 25 — Where a CII operator violates the provisions of Articles 14 or 15 of these Regulations, the relevant competent department shall, in accordance with its functions and duties, order the operator to take corrective action and issue a warning. Where the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed on the operator, and the persons directly in charge shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 26 — Where a CII operator violates the provisions of Article 12 of these Regulations by using network products and services that have not undergone a security review or fail to pass a security review, the relevant competent department shall, in accordance with its functions and duties, order the operator to cease the use and impose a fine of not less than one time but not more than 10 times the purchase amount, and impose a fine of not less than RMB 10,000 but not more than RMB 100,000 on the persons directly in charge and other persons directly responsible.

Article 27 — Where a network product or service provider, in the course of providing products or services for CII, commits acts endangering CII security, such as illegally implanting backdoors or malicious programs, the relevant competent department shall impose punishment in accordance with the law.

Article 28 — Where, in violation of the provisions of these Regulations, damage is caused to CII or national security is endangered, and the violation constitutes a crime, criminal liability shall be pursued in accordance with the law. Where the violation does not constitute a crime, the public security department and the national security department shall impose punishment in accordance with the law.

Chapter VI — Supplementary Provisions

Article 29 — These Regulations shall not apply to the security protection of CII in military networks and networks involving State secrets.

Article 30 — Security protection of CII in secret-related networks shall be governed by the provisions of laws and administrative regulations on the protection of State secrets.

Article 31 — These Regulations shall take effect as of September 1, 2021.

Source: https://www.danyoungcpa.com/critical-information-infrastructure-security-protection-measures-2021/

Disclaimer: This English translation is provided for reference and informational purposes only. While every effort has been made to ensure accuracy, it is not an official translation and may contain errors or omissions. The official Chinese text as published by the State Council of the People's Republic of China shall prevail in all legal matters. Dan Young Business Consultancy makes no warranty, express or implied, regarding the accuracy, completeness, or fitness for any particular purpose of this translation. Users should consult qualified legal professionals for advice on specific legal matters and refer to the official Chinese text for authoritative interpretation. This translation does not constitute legal advice.