Regulation on the Protection of Critical Information Infrastructure of the PRC

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 — Identification of Critical Information Infrastructure 2

Chapter III — Obligations of Operators 3

Chapter IV — Safeguard and Promotion 4

Chapter V — Legal Liability 5

Chapter VI — Supplementary Provisions 6

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

Table of Contents

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

Chapter I — General Provisions

Article 1 — These Regulations are enacted in accordance with the Cybersecurity Law of the People's Republic of China for the purposes of ensuring the security of critical information infrastructure, and safeguarding national security, the national economy, people's livelihoods, and the public interest.

Article 2 — For the purposes of these Regulations, "critical information infrastructure" refers to important network facilities and information systems in important industries and fields such as public telecommunications and information services, energy, transport, water conservancy, finance, public services, e-government, and the defense science, technology, and industry sector, as well as other important network facilities and information systems that, in the event of damage, loss of function, or data leakage, may seriously jeopardize national security, the national economy, people's livelihoods, or the public interest.

Source: https://www.danyoungcpa.com/regulation-protection-critical-information-infrastructure-prc-2021/

Article 3 — Work relating to the protection of critical information infrastructure shall adhere to the leadership of the Communist Party of China, implement a national security approach, and be carried out under the principles of overall planning and coordination, division of responsibilities and close cooperation, integrated leadership and industry and sector-based management, and equal emphasis on protection and development.

Article 4 — The Cyberspace Administration of China shall be responsible for the overall coordination and supervision of work related to the protection of critical information infrastructure throughout the country. The public security department of the State Council shall be responsible for guiding and supervising the security protection of critical information infrastructure. The state secret-keeping administration department of the State Council shall be responsible for guiding and supervising secrecy protection work related to critical information infrastructure. Competent departments and supervision and administration departments of all industries and fields related to critical information infrastructure under the State Council (hereinafter referred to as "protection work departments") shall, in accordance with their duties, be respectively responsible for the security protection of critical information infrastructure within their respective industries and fields. Other relevant departments of the State Council shall, in accordance with the provisions, assume relevant responsibilities in the security protection of critical information infrastructure. Local people's governments at all levels shall, in accordance with relevant provisions, organize and carry out relevant work related to the protection of critical information infrastructure within their administrative regions.

Article 5 — The state shall implement a system of priority protection, focused protection, and overall protection for critical information infrastructure, and take measures such as monitoring, early warning, emergency response, and information sharing to cope with cybersecurity risks and threats.

Article 6 — Operators of critical information infrastructure shall, in accordance with the provisions of these Regulations, the Cybersecurity Law, and other relevant laws and administrative regulations, and under the guidance of protection work departments, establish and improve security protection systems, fulfill security protection responsibilities, and accept the supervision and management of the state and the public.

Article 7 — Units and individuals that have made outstanding contributions in the protection of critical information infrastructure, or that have committed significant achievements, shall be commended and rewarded in accordance with relevant national provisions.

Chapter II — Identification of Critical Information Infrastructure

Article 8 — Important industries and fields referred to in these Regulations include important network facilities and information systems in such critical sectors as public telecommunications and information services, energy, transport, water conservancy, finance, public services, e-government, and the defense science, technology, and industry sector.

Article 9 — Protection work departments shall, in accordance with rules for the identification of critical information infrastructure formulated by the Cyberspace Administration of China in conjunction with the relevant departments, organize and carry out identification of critical information infrastructure within their respective industries and fields. The identification results shall be promptly notified to the operators of the relevant critical information infrastructure and reported to the public security department of the State Council.

Article 10 — In identifying critical information infrastructure, the following factors shall be taken into account:

(1) — The degree of importance of the network facility, information system, and such to the critical core operations of the industry or field;

(2) — The degree of damage that may be caused to national security, the national economy, people's livelihoods, or the public interest in the event of damage to, loss of function of, or data leakage from the network facility, information system, etc.;

Source: https://www.danyoungcpa.com/regulation-protection-critical-information-infrastructure-prc-2021/

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

Article 11 — Upon a substantial change in circumstances that may affect the identification result, protection work departments shall re-organize identification of critical information infrastructure and promptly notify operators of the re-identification result.

Chapter III — Obligations of Operators

Article 12 — Operators of critical information infrastructure shall establish and improve cybersecurity protection systems and responsibility systems to ensure the security and stable operation of critical information infrastructure. They shall designate a principal person responsible for the security and operation of critical information infrastructure and conduct a security assessment of the principal person responsible and key personnel positions; where a person is found unsuitable for the position, the operator shall make adjustments in a timely manner.

Article 13 — Operators shall establish dedicated security management bodies and provide guarantees for personnel and funds necessary for the operation of such bodies. The dedicated security management body shall perform the following duties:

(1) — Establish and improve network security management, evaluation, and assessment systems, and formulate a security protection plan for critical information infrastructure;

(2) — Organize and promote education, training, and assessment of cybersecurity protection capabilities;

(3) — Formulate emergency plans for cybersecurity incidents, conduct emergency drills on a regular basis, and handle cybersecurity incidents;

(4) — Determine cybersecurity positions and evaluate the security backgrounds of persons to be employed for such positions;

(5) — Provide security management for the design, construction, operation, and maintenance of and services for critical information infrastructure;

(6) — Conduct real-time monitoring and security assessment of the cybersecurity vulnerabilities and security incidents related to critical information infrastructure, and make recommendations for the improvement of security protection measures;

(7) — Fulfill other duties relating to the security protection of critical information infrastructure as required by law.

Article 14 — Operators shall fulfill the following security obligations:

(1) — Establish and improve cybersecurity monitoring and early warning systems, and take immediate measures to investigate and remediate cybersecurity vulnerabilities, threats, and risks;

(2) — Conduct regular cybersecurity inspections, risk assessments, and rectification;

(3) — Keep logs of network operations, security incidents, and other relevant network logs for not less than six months in accordance with provisions;

(4) — Implement data classification, grading, and protection and take necessary technical measures for protection of important data and core data such as encrypted storage and authentication control;

(5) — Formulate contingency plans for major cybersecurity incidents and report to protection work departments for record-filing in a timely manner;

(6) — Prioritize the procurement of secure and reliable network products and services; where network products and services may affect national security, they shall pass the security review under the national security review system;

Source: https://www.danyoungcpa.com/regulation-protection-critical-information-infrastructure-prc-2021/

(7) — Sign a security protection agreement or a confidentiality agreement with service providers to clarify security obligations and liabilities;

(8) — Report cybersecurity incidents to protection work departments and public security authorities in accordance with provisions.

Article 15 — Where operators purchase network products and services, they shall, in accordance with relevant national provisions, sign a security protection agreement or confidentiality agreement with the providers of network products and services to clarify technical support, security protection, confidentiality, and other obligations and responsibilities of the providers, and supervise the performance thereof.

Article 16 — Operators shall, at their own or by commissioning a cybersecurity service institution, conduct a cybersecurity inspection and risk assessment of critical information infrastructure at least once a year, detect and remediate security issues in a timely manner, and report the results to protection work departments in accordance with protection work department requirements.

Article 17 — In the event of a merger, division, dissolution, or other major change to critical information infrastructure, operators shall promptly report to protection work departments and dispose of critical information infrastructure in accordance with the requirements of protection work departments to ensure security.

Article 18 — Operators shall give priority to the procurement of secure and reliable network products and services. Where the network products and services provided may affect national security, a security review shall be conducted in accordance with the Measures for Cybersecurity Review.

Article 19 — Where operators need to store personal information or important data collected and generated within the territory of the People's Republic of China abroad, a security assessment shall be conducted in accordance with national provisions. Where laws and administrative regulations provide otherwise, such provisions shall prevail.

Chapter IV — Safeguard and Promotion

Article 20 — Protection work departments shall formulate security protection plans for critical information infrastructure within their respective industries and fields and organize and guide the implementation of such plans by operators within their respective industries and fields.

Article 21 — Protection work departments shall establish and improve a cybersecurity monitoring and early warning system for critical information infrastructure within their respective industries and fields, keep abreast of the operational status, security situation, and real-time threat information of critical information infrastructure, promptly circulate early warning information, and guide operators in conducting security protection work.

Article 22 — Protection work departments shall organize and carry out cybersecurity inspections and testing of critical information infrastructure within their respective industries and fields on a regular basis, instruct operators to identify security risks and vulnerabilities, make rectifications, and take improvement measures. Such inspections and testing shall not charge fees or require operators to purchase designated brands or products or services from designated entities.

Article 23 — The Cyberspace Administration of China shall, in conjunction with the public security department of the State Council, protection work departments, and other relevant departments, establish and improve mechanisms for sharing cybersecurity information, circulate cybersecurity threat information in a timely manner, and use such information to conduct analysis, research, and judgment, report to the state and circulate the same, so as to provide support for the security protection of critical information infrastructure.

Article 24 — Protection work departments shall establish and improve emergency response mechanisms for cybersecurity incidents in critical information infrastructure within their respective industries and fields, formulate emergency plans, organize emergency drills on a regular basis, and guide and coordinate operators in performing emergency response work related to cybersecurity incidents.

Article 25 — The state encourages and supports scientific research institutions, institutions of higher learning, enterprises, and other entities to conduct research on cybersecurity technologies, provide technical and human resources support for the security protection of critical information infrastructure, and cultivate specialized cybersecurity personnel.

Article 26 — The state encourages and supports cybersecurity service institutions to participate in relevant work of critical information infrastructure security protection through providing security monitoring, risk assessment, and early warning services. Cybersecurity service institutions shall fulfill confidentiality obligations and may not disclose, sell, or illegally provide to others information or materials obtained during the performance of their work.

Chapter V — Legal Liability

Article 27 — Where an operator violates Article 12 of these Regulations by failing to establish or improve a cybersecurity protection system or responsibility system, or failing to designate a principal person responsible and conduct a security assessment of such person and key personnel positions, the relevant protection work department shall, according to its duties, order it to take corrective action and issue a warning; where it refuses to take corrective action, or causes harm or other consequences as a result, a fine of not less than RMB 100,000 but not more than RMB 1,000,000 shall be imposed, and the directly responsible person in charge shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 28 — Where an operator violates the provisions of Articles 14 and 15 of these Regulations by failing to fulfill statutory security protection duties, the relevant protection work department shall, according to its duties, order it to take corrective action and issue a warning; where it refuses to take corrective action, or causes harm or other consequences as a result, a fine of not less than RMB 100,000 but not more than RMB 1,000,000 shall be imposed, and the directly responsible person in charge shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 29 — Where an operator violates these Regulations in the course of any cybersecurity inspection or risk assessment of critical information infrastructure, and the circumstances are serious, the relevant protection work department shall, according to its duties, order it to take corrective action and issue a warning, and may impose a fine of not less than RMB 50,000 but not more than RMB 500,000.

Article 30 — Where any protection work department or relevant department or any staff member thereof engages in any of the following conduct in the course of security protection of critical information infrastructure, the directly responsible person in charge and other directly liable persons shall be subject to disciplinary action in accordance with law:

(1) — Failing to perform the duties of security protection of critical information infrastructure, dereliction of duty, or engaging in malpractice for personal gain;

(2) — Abusing authority, neglecting duties, or committing fraud for personal gain in the course of carrying out inspections and testing, identification of critical information infrastructure, or other work;

(3) — Disclosing, selling, or illegally providing to others information or materials obtained in the course of performance of duties;

(4) — Other conduct involving failure to perform statutory duties in accordance with the law.

Article 31 — Where violations of these Regulations constitute an offense constituting a crime, criminal liability shall be pursued in accordance with law; where harm is caused to the person or property of others,

Source: https://www.danyoungcpa.com/regulation-protection-critical-information-infrastructure-prc-2021/

civil liability shall be borne in accordance with law.

Chapter VI — Supplementary Provisions

Article 32 — For the purposes of these Regulations, "operators of critical information infrastructure" refers to the owners, administrators, and service providers of critical information infrastructure.

Article 33 — The security protection of critical information infrastructure involved in the storage, processing of state secret information shall also comply with the provisions of laws and administrative regulations on state secret protection.

Article 34 — The security protection of critical information infrastructure in the military field shall be prescribed by the Central Military Commission.

Article 35 — These Regulations shall come 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. In the event of any discrepancy between this English version and the original Chinese text, the original Chinese text shall prevail. Readers should consult qualified legal professionals for advice on specific legal matters. Dan Young Business Consultancy makes no representations or warranties as to the accuracy or completeness of this translation and assumes no liability for any reliance placed upon it.

Source: https://www.danyoungcpa.com/regulation-protection-critical-information-infrastructure-prc-2021/