Cybersecurity Law 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 — Cybersecurity Support and Promotion 3

Chapter III — Network Operation Security 4

Section 1 — General Provisions 4

Section 2 — Security of the Operation of Critical Information Infrastructure 6

Chapter IV — Network Information Security 7

Chapter V — Monitoring, Early Warning and Emergency Response 8

Chapter VI — Legal Liability 9

Chapter VII — Supplementary Provisions 13

Adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress on November 7, 2016

Amended in accordance with the Decision on Amending the Cybersecurity Law of the People's Republic of China adopted at the 18th Session of the Standing Committee of the Fourteenth National People's Congress on October 28, 2025

Effective: June 1, 2017; amendment effective January 1, 2026

Table of Contents

- Chapter I — General Provisions
- Chapter II — Cybersecurity Support and Promotion
- Chapter III — Network Operation Security
- Chapter IV — Network Information Security
- Chapter V — Monitoring, Early Warning and Emergency Response
- Chapter VI — Legal Liability
- Chapter VII — Supplementary Provisions

Chapter I — General Provisions

Article 1 — This Law is enacted for the purposes of ensuring cybersecurity, safeguarding cyberspace sovereignty, national security and public interests, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization.

Article 2 — This Law applies to the construction, operation, maintenance and use of networks within the territory of the People's Republic of China, as well as to the supervision and administration of cybersecurity.

Article 3 — Cybersecurity work shall uphold the leadership of the Communist Party of China, implement a holistic approach to national security, coordinate development and security, and advance the building of a strong cyber nation.

Article 4 — The state shall attach equal importance to cybersecurity and informatization development, follow the principles of active utilization, scientific development, lawful administration and ensured security, promote the construction of and interconnection among network infrastructure, encourage innovation and application of network technology, support the cultivation of cybersecurity professionals, establish and improve the cybersecurity guarantee system, and enhance cybersecurity protection capabilities.

Article 5 — The state shall formulate and continuously improve the cybersecurity strategy, define the basic requirements and principal objectives for ensuring cybersecurity, and put forward cybersecurity policies, work tasks and measures in key areas.

Article 6 — The state shall take measures to monitor, defend against and respond to cybersecurity risks and threats originating from within or outside the territory of the People's Republic of China, protect critical information infrastructure from attack, intrusion, interference and destruction, punish illegal and criminal network activities in accordance with the law, and maintain security and order in cyberspace.

Article 7 — The state shall advocate honest, trustworthy, healthy and civilized network conduct, promote the dissemination of core socialist values, take measures to raise the cybersecurity awareness and level of the whole society, and create a sound environment in which the whole society jointly participates in promoting cybersecurity.

Article 8 — The state shall actively carry out international exchanges and cooperation in cyberspace governance, research and development of network technology and standard-setting, and the combating of illegal and criminal network activities, promote the building of a peaceful, secure, open and cooperative cyberspace, and establish a multilateral, democratic and transparent network governance system.

Article 9 — The state cyberspace administration department shall be responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration. The telecommunications administration department, the public security department and other relevant organs of the State Council shall, in accordance with this Law and other relevant laws and administrative regulations, be responsible for cybersecurity protection, supervision and administration within their respective scope of duties.

The cybersecurity protection, supervision and administration duties of the relevant departments of local people's governments at or above the county level shall be determined in accordance with the relevant provisions of the state.

Article 10 — When operating and providing services, network operators shall abide by laws and administrative regulations, respect social morality and business ethics, be honest and trustworthy, fulfill their cybersecurity protection obligations, accept supervision by the government and society, and bear social responsibility.

Article 11 — In building or operating networks, or providing services through networks, technical measures and other necessary measures shall be taken in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, so as to ensure the secure and stable operation of networks, effectively respond to cybersecurity incidents, prevent illegal and criminal network

activities, and maintain the integrity, confidentiality and availability of network data.

Article 12 — Network-related industry organizations shall, in accordance with their charters, strengthen industry self-discipline, formulate cybersecurity codes of conduct, guide their members in strengthening cybersecurity protection and raising cybersecurity protection levels, and promote the sound development of the industry.

Article 13 — The state shall protect the right of citizens, legal persons and other organizations to use networks in accordance with the law, promote the popularization of network access, improve network service levels, provide society with secure and convenient network services, and guarantee the lawful, orderly and free flow of network information in accordance with the law.

Any individual or organization using a network shall abide by the Constitution and laws, observe public order and respect social morality, and shall not endanger cybersecurity, or use the network to engage in activities endangering national security, honor and interests; inciting subversion of state power or the overthrow of the socialist system; inciting secession of the state or undermining national unity; propagating terrorism or extremism; propagating ethnic hatred or ethnic discrimination; disseminating violent or pornographic information; fabricating or disseminating false information to disrupt economic and social order; or infringing upon the reputation, privacy, intellectual property rights or other lawful rights and interests of others.

Article 14 — The state shall support the research and development of network products and services conducive to the healthy growth of minors, punish in accordance with the law activities that use the network to endanger the physical and mental health of minors, and provide minors with a safe and healthy network environment.

Article 15 — Any individual or organization shall have the right to report conduct endangering cybersecurity to the cyberspace administration, telecommunications, public security and other departments. The department receiving a report shall handle it in a timely manner in accordance with the law; where the report does not fall within its scope of duties, it shall promptly transfer it to the department with the authority to handle it.

The relevant departments shall keep confidential the relevant information of the reporter and protect the lawful rights and interests of the reporter.

Chapter II — Cybersecurity Support and Promotion

Article 16 — The state shall establish and improve the cybersecurity standard system. The standardization administrative department of the State Council and other relevant departments of the State Council shall, in accordance with their respective duties, organize the formulation and timely revision of national standards and industry standards relating to cybersecurity administration and the security of network products, services and operations.

The state shall support enterprises, research institutions, institutions of higher learning and network-related industry organizations in participating in the formulation of national standards and industry standards on cybersecurity.

Article 17 — The State Council and the people's governments of provinces, autonomous regions and municipalities directly under the Central Government shall make overall plans, increase investment, support key cybersecurity technology industries and projects, support the research, development and application of cybersecurity technology, promote secure and trustworthy network products and services, protect intellectual property rights in network technology, and support enterprises, research institutions and institutions of higher learning in participating in national cybersecurity technology innovation projects.

Article 18 — The state shall promote the establishment of a cybersecurity social service system, and encourage relevant enterprises and institutions to carry out security services such as cybersecurity

certification, testing and risk assessment.

Article 19 — The state shall encourage the development of technology for the protection and utilization of network data security, promote the opening of public data resources, and advance technological innovation and economic and social development.

Article 20 — The state shall support basic theoretical research on artificial intelligence and research and development of key technologies such as algorithms, promote the construction of infrastructure such as training data resources and computing power, improve artificial intelligence ethics standards, strengthen risk monitoring, assessment and safety regulation, and promote the healthy application and development of artificial intelligence.

The state shall support innovation in cybersecurity administration methods and the use of new technologies such as artificial intelligence to raise the level of cybersecurity protection.

Article 21 — People's governments at all levels and their relevant departments shall organize and carry out regular cybersecurity publicity and education, and guide and supervise the relevant units in doing a good job of cybersecurity publicity and education.

Mass media shall carry out targeted cybersecurity publicity and education for the public.

Article 22 — The state shall support enterprises and institutions of higher learning, vocational schools and other education and training institutions in carrying out cybersecurity-related education and training, cultivate cybersecurity professionals through multiple means, and promote exchanges among cybersecurity professionals.

Chapter III — Network Operation Security

Section 1 — General Provisions

Article 23 — The state shall implement a system of graded protection for cybersecurity. Network operators shall, in accordance with the requirements of the graded protection system for cybersecurity, fulfill the following security protection obligations to ensure that networks are protected from interference, destruction or unauthorized access, and to prevent network data from being leaked, stolen or tampered with:

(1) formulating internal security management systems and operating procedures, designating persons responsible for cybersecurity, and implementing cybersecurity protection responsibilities;

(2) taking technical measures to prevent computer viruses, network attacks, network intrusions and other acts endangering cybersecurity;

(3) taking technical measures to monitor and record network operation status and cybersecurity incidents, and retaining relevant network logs for no less than six months in accordance with provisions;

(4) taking measures such as data classification, backup of important data and encryption; and

(5) other obligations prescribed by laws and administrative regulations.

Article 24 — Network products and services shall comply with the mandatory requirements of the relevant national standards. Providers of network products and services shall not set up malicious programs; upon discovering security defects, vulnerabilities or other risks in their network products or services, they shall immediately take remedial measures, promptly notify users in accordance with provisions, and report to the relevant competent departments.

Providers of network products and services shall continuously provide security maintenance for their products and services, and shall not terminate the provision of security maintenance within the period prescribed by provisions or agreed upon by the parties.

Source: https://www.danyoungcpa.com/cybersecurity-law-prc-2025-revision/

Where network products or services have the function of collecting user information, their providers shall expressly inform users and obtain their consent; where personal information of users is involved, the provisions of this Law and the relevant laws and administrative regulations on the protection of personal information shall also be observed.

Article 25 — Network critical equipment and special-purpose cybersecurity products shall be sold or provided only after passing security certification by qualified institutions or conforming to security testing requirements. The state cyberspace administration department shall, jointly with the relevant departments of the State Council, formulate and publish catalogs of network critical equipment and special-purpose cybersecurity products, and promote mutual recognition of security certification and security testing results, so as to avoid repeated certification and testing.

Article 26 — When handling network access or domain name registration services for users, handling procedures for fixed-line or mobile telephones or other network access, or providing services such as information publishing or instant messaging for users, network operators shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where a user does not provide real identity information, the network operator shall not provide the relevant services to the user.

The state shall implement a strategy for trusted online identities, support the research and development of secure and convenient electronic identity authentication technology, and promote mutual recognition among different electronic identity authentications.

Article 27 — Network operators shall formulate emergency response plans for cybersecurity incidents and promptly handle security risks such as system vulnerabilities, computer viruses, network attacks and network intrusions; when an incident endangering cybersecurity occurs, they shall immediately initiate the emergency response plan, take corresponding remedial measures, and report to the relevant competent departments in accordance with provisions.

Article 28 — Activities such as carrying out cybersecurity certification, testing and risk assessment, and publicly disclosing cybersecurity information such as system vulnerabilities, computer viruses, network attacks and network intrusions shall comply with the relevant provisions of the state.

Article 29 — No individual or organization may engage in activities endangering cybersecurity such as illegally intruding into another's network, interfering with the normal functioning of another's network, or stealing network data; may not provide programs or tools specifically designed to engage in activities endangering cybersecurity such as network intrusion, interference with normal network functions and protective measures, or theft of network data; and may not provide technical support, advertising promotion, payment and settlement or other assistance to others whom they know to be engaging in activities endangering cybersecurity.

Article 30 — Network operators shall provide technical support and assistance to public security organs and state security organs in their lawful activities of safeguarding national security and investigating crimes.

Article 31 — The state shall support cooperation among network operators in the collection, analysis, notification and emergency response of cybersecurity information, so as to improve the security assurance capabilities of network operators.

Relevant industry organizations shall establish and improve cybersecurity protection standards and coordination mechanisms for their respective industries, strengthen the analysis and assessment of cybersecurity risks, regularly issue risk warnings to their members, and support and assist their members in responding to cybersecurity risks.

Article 32 — Information obtained by the cyberspace administration department and relevant departments in the performance of their cybersecurity protection duties may be used only for the needs of maintaining

cybersecurity, and may not be used for other purposes.

Section 2 — Security of the Operation of Critical Information Infrastructure

Article 33 — The state shall, on the basis of the graded protection system for cybersecurity, provide key protection for critical information infrastructure in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government, as well as other critical information infrastructure which, once damaged, disabled or subject to data leakage, may seriously endanger national security, the national economy and people's livelihood, or public interests. The specific scope and security protection measures for critical information infrastructure shall be formulated by the State Council.

The state shall encourage network operators other than those of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

Article 34 — Departments responsible for the security protection of critical information infrastructure shall, in accordance with the division of duties prescribed by the State Council, respectively prepare and organize the implementation of critical information infrastructure security plans for their respective industries and fields, and guide and supervise the security protection of the operation of critical information infrastructure.

Article 35 — In constructing critical information infrastructure, it shall be ensured that it has the performance to support stable and continuous business operation, and that security technical measures are planned, constructed and used simultaneously.

Article 36 — In addition to the provisions of Article 23 of this Law, operators of critical information infrastructure shall also fulfill the following security protection obligations:

(1) establishing special security management institutions and designating persons responsible for security management, and conducting security background checks on such persons and personnel in key positions;

(2) regularly providing cybersecurity education, technical training and skills assessment for employees;

(3) conducting disaster recovery backup for important systems and databases;

(4) formulating emergency response plans for cybersecurity incidents and conducting regular drills; and

(5) other obligations prescribed by laws and administrative regulations.

Article 37 — Where the procurement of network products and services by an operator of critical information infrastructure may affect national security, it shall undergo a national security review organized by the state cyberspace administration department jointly with the relevant departments of the State Council.

Article 38 — In procuring network products and services, operators of critical information infrastructure shall, in accordance with provisions, sign security and confidentiality agreements with providers, specifying security and confidentiality obligations and responsibilities.

Article 39 — Personal information and important data collected and generated by operators of critical information infrastructure during their operations within the territory of the People's Republic of China shall be stored within the territory. Where it is truly necessary to provide such information or data abroad for business needs, a security assessment shall be conducted in accordance with the measures formulated by the state cyberspace administration department jointly with the relevant departments of the State Council; where laws or administrative regulations provide otherwise, such provisions shall prevail.

Article 40 — Operators of critical information infrastructure shall, on their own or by entrusting cybersecurity service institutions, conduct at least one testing and assessment of the security of their networks and possible risks each year, and submit the testing and assessment results and improvement measures to the department responsible for the security protection of critical information infrastructure.

Article 41 — The state cyberspace administration department shall coordinate the relevant departments in taking the following measures for the security protection of critical information infrastructure:

(1) conducting spot checks and testing of the security risks of critical information infrastructure and proposing improvement measures, and, where necessary, entrusting cybersecurity service institutions to conduct testing and assessment of the security risks existing in networks;

(2) regularly organizing operators of critical information infrastructure to conduct cybersecurity emergency response drills, so as to improve their ability to respond to cybersecurity incidents and their coordination and cooperation capabilities;

(3) promoting the sharing of cybersecurity information among relevant departments, operators of critical information infrastructure, and relevant research institutions and cybersecurity service institutions; and

(4) providing technical support and assistance for emergency response to cybersecurity incidents and the restoration of network functions.

Chapter IV — Network Information Security

Article 42 — Network operators shall strictly keep confidential the user information they collect, and establish and improve user information protection systems.

When processing personal information, network operators shall comply with the provisions of this Law and laws and administrative regulations such as the Civil Code of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China.

Article 43 — When collecting and using personal information, network operators shall follow the principles of lawfulness, legitimacy and necessity, disclose the rules for collection and use, expressly indicate the purpose, method and scope of the collection and use of information, and obtain the consent of the persons whose information is collected.

Network operators shall not collect personal information unrelated to the services they provide, shall not collect or use personal information in violation of the provisions of laws and administrative regulations or the agreement between the parties, and shall process the personal information they have stored in accordance with the provisions of laws and administrative regulations and the agreement with users.

Article 44 — Network operators shall not disclose, tamper with or destroy the personal information they collect; and shall not provide personal information to others without the consent of the persons whose information is collected, except where the information has been processed so that specific individuals cannot be identified and cannot be restored.

Network operators shall take technical measures and other necessary measures to ensure the security of the personal information they collect and prevent information from being leaked, destroyed or lost. Where personal information is or may be leaked, destroyed or lost, they shall immediately take remedial measures, promptly notify users in accordance with provisions, and report to the relevant competent departments.

Article 45 — Where an individual discovers that a network operator has collected or used his or her personal information in violation of the provisions of laws and administrative regulations or the agreement between the parties, he or she shall have the right to require the network operator to delete his or her personal information; where the individual discovers that the personal information collected or stored by the network operator is erroneous, he or she shall have the right to require the network operator to correct it. The network operator shall take measures to delete or correct it.

Article 46 — No individual or organization may steal or obtain personal information by other illegal means, or illegally sell or illegally provide personal information to others.

Article 47 — Departments legally responsible for cybersecurity supervision and administration and their staff shall strictly keep confidential the personal information, privacy and trade secrets they learn in the performance of their duties, and shall not disclose, sell or illegally provide such information to others.

Article 48 — Any individual or organization shall be responsible for their own conduct in using networks, and shall not set up websites or communication groups for committing fraud, teaching criminal methods, or producing or selling prohibited or controlled articles, or other illegal or criminal activities; and shall not use networks to publish information relating to the commission of fraud, the production or sale of prohibited or controlled articles, or other illegal or criminal activities.

Article 49 — Network operators shall strengthen the management of information published by their users. Upon discovering information the publication or transmission of which is prohibited by laws or administrative regulations, they shall immediately stop transmitting such information, take disposal measures such as elimination to prevent the information from spreading, preserve relevant records, and report to the relevant competent departments.

Article 50 — Electronic information sent and application software provided by any individual or organization shall not contain malicious programs or information the publication or transmission of which is prohibited by laws or administrative regulations.

Providers of electronic information sending services and application software downloading services shall fulfill their security management obligations; where they know that their users have committed the acts described in the preceding paragraph, they shall stop providing services, take disposal measures such as elimination, preserve relevant records, and report to the relevant competent departments.

Article 51 — Network operators shall establish systems for complaints and reports regarding network information security, publish information such as complaint and reporting methods, and promptly accept and handle complaints and reports concerning network information security.

Network operators shall cooperate with the supervision and inspection lawfully conducted by the cyberspace administration department and relevant departments.

Article 52 — The state cyberspace administration department and relevant departments shall, in accordance with the law, fulfill their duties of supervising and administering network information security; upon discovering information the publication or transmission of which is prohibited by laws or administrative regulations, they shall require network operators to stop transmission, take disposal measures such as elimination, and preserve relevant records; with respect to such information originating from outside the territory of the People's Republic of China, they shall notify the relevant institutions to take technical measures and other necessary measures to block its dissemination.

Chapter V — Monitoring, Early Warning and Emergency Response

Article 53 — The state shall establish a cybersecurity monitoring, early warning and information notification system. The state cyberspace administration department shall coordinate the relevant departments in strengthening the collection, analysis and notification of cybersecurity information, and uniformly publish cybersecurity monitoring and early warning information in accordance with provisions.

Article 54 — Departments responsible for the security protection of critical information infrastructure shall establish and improve cybersecurity monitoring, early warning and information notification systems for their respective industries and fields, and submit cybersecurity monitoring and early warning information in accordance with provisions.

Article 55 — The state cyberspace administration department shall coordinate the relevant departments in establishing and improving cybersecurity risk assessment and emergency response working mechanisms, formulating emergency response plans for cybersecurity incidents, and organizing regular drills.

Departments responsible for the security protection of critical information infrastructure shall formulate emergency response plans for cybersecurity incidents for their respective industries and fields, and organize regular drills.

Emergency response plans for cybersecurity incidents shall classify cybersecurity incidents according to factors such as the degree of harm and scope of impact after the occurrence of an incident, and prescribe corresponding emergency response measures.

Article 56 — When the risk of a cybersecurity incident increases, the relevant departments of people's governments at or above the provincial level shall, in accordance with the prescribed authority and procedures and based on the characteristics of the cybersecurity risk and the possible harm it may cause, take the following measures:

(1) requiring the relevant departments, institutions and personnel to promptly collect and report relevant information and strengthen the monitoring of cybersecurity risks;

(2) organizing the relevant departments, institutions and professionals to analyze and assess cybersecurity risk information and predict the possibility of occurrence, scope of impact and degree of harm of incidents; and

(3) issuing cybersecurity risk warnings to the public and publishing measures to avoid and mitigate harm.

Article 57 — When a cybersecurity incident occurs, the emergency response plan for cybersecurity incidents shall be initiated immediately; the cybersecurity incident shall be investigated and assessed; network operators shall be required to take technical measures and other necessary measures to eliminate security hazards and prevent the harm from expanding; and warning information relating to the public shall be promptly published.

Article 58 — Where the relevant departments of people's governments at or above the provincial level discover, in the performance of their cybersecurity supervision and administration duties, that a network has relatively serious security risks or that a security incident has occurred, they may, in accordance with the prescribed authority and procedures, hold regulatory interviews with the legal representative or principal person in charge of the operator of the network. The network operator shall take measures in accordance with the requirements to carry out rectification and eliminate the hazards.

Article 59 — Where a cybersecurity incident gives rise to an emergency or a production safety accident, it shall be handled in accordance with the provisions of the Emergency Response Law of the People's Republic of China, the Work Safety Law of the People's Republic of China and other relevant laws and administrative regulations.

Article 60 — Where necessary for safeguarding national security and social public order and for handling major emergencies involving public security, temporary measures such as restrictions on network communications may be taken in specific areas upon decision or approval by the State Council.

Chapter VI — Legal Liability

Article 61 — Where a network operator fails to fulfill the cybersecurity protection obligations prescribed in Articles 23 and 27 of this Law, the relevant competent department shall order it to make corrections, give it a warning, and may impose a fine of not less than RMB 10,000 but not more than RMB 50,000; where it refuses to make corrections or causes consequences endangering cybersecurity, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and the persons directly in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Where an operator of critical information infrastructure fails to fulfill the cybersecurity protection obligations prescribed in Articles 35, 36, 38 and 40 of this Law, the relevant competent department shall order it to make corrections, give it a warning, and may impose a fine of not less than RMB 50,000 but not more than RMB

100,000; where it refuses to make corrections or causes consequences endangering cybersecurity, 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 and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Where any of the acts described in the preceding two paragraphs causes serious consequences endangering cybersecurity such as large-scale data leakage or loss of partial functionality of critical information infrastructure, the relevant competent department shall impose a fine of not less than RMB 500,000 but not more than RMB 2,000,000, and the persons directly in charge and other directly responsible persons shall be fined not less than RMB 50,000 but not more than RMB 200,000; where it causes particularly serious consequences endangering cybersecurity such as loss of principal functionality of critical information infrastructure, a fine of not less than RMB 2,000,000 but not more than RMB 10,000,000 shall be imposed, and the persons directly in charge and other directly responsible persons shall be fined not less than RMB 200,000 but not more than RMB 1,000,000.

Article 62 — Where any of the following acts is committed in violation of paragraphs 1 and 2 of Article 24 and paragraph 1 of Article 50 of this Law, the relevant competent department shall order corrections and give a warning; where corrections are refused or consequences endangering cybersecurity are caused, a fine of not less than RMB 50,000 but not more than RMB 500,000 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:

(1) setting up malicious programs;

(2) failing to immediately take remedial measures for security defects, vulnerabilities or other risks in their products or services, or failing to promptly notify users and report to the relevant competent departments in accordance with provisions; or

(3) terminating the provision of security maintenance for their products or services without authorization.

Where the acts described in items (1) and (2) of the preceding paragraph cause the consequences prescribed in paragraph 3 of Article 61 of this Law, penalties shall be imposed in accordance with the provisions of that paragraph.

Article 63 — Where, in violation of Article 25 of this Law, network critical equipment or special-purpose cybersecurity products that have not undergone security certification or security testing, or that have failed security certification or do not conform to security testing requirements, are sold or provided, the relevant competent department shall order the cessation of sale or provision, give a warning, and confiscate illegal gains; where there are no illegal gains or the illegal gains are less than RMB 100,000, a fine of not less than RMB 20,000 but not more than RMB 100,000 shall be imposed concurrently; where the illegal gains are RMB 100,000 or more, a fine of not less than one time but not more than five times the illegal gains shall be imposed concurrently; where the circumstances are serious, the relevant competent department may also order suspension of relevant business, suspension of business for rectification, revocation of the relevant business license or revocation of the business license. Where laws or administrative regulations provide otherwise, such provisions shall prevail.

Article 64 — Where a network operator, in violation of paragraph 1 of Article 26 of this Law, fails to require users to provide real identity information, or provides relevant services to users who do not provide real identity information, the relevant competent department shall order it to make corrections; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and the relevant competent department may also order suspension of relevant business, suspension of business for rectification, closure of the website or application, revocation of the relevant business license or revocation of the business license, and the persons directly in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 65 — Where, in violation of Article 28 of this Law, activities such as cybersecurity certification, testing and risk assessment are carried out, or cybersecurity information such as system vulnerabilities, computer viruses, network attacks and network intrusions is publicly disclosed, the relevant competent department shall order corrections, give a warning, and may impose a fine of not less than RMB 10,000 but not more than RMB 100,000; where corrections are refused or 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 relevant competent department may also order suspension of relevant business, suspension of business for rectification, closure of the website or application, revocation of the relevant business license or revocation of the business license, and the persons directly in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Where the acts described in the preceding paragraph cause the consequences prescribed in paragraph 3 of Article 61 of this Law, penalties shall be imposed in accordance with the provisions of that paragraph.

Article 66 — Where a person, in violation of Article 29 of this Law, engages in activities endangering cybersecurity, provides programs or tools specifically designed to engage in activities endangering cybersecurity, or provides technical support, advertising promotion, payment and settlement or other assistance to others engaging in activities endangering cybersecurity, and the act does not constitute a crime, the public security organ shall confiscate the illegal gains and impose detention of not more than five days, and may concurrently impose a fine of not less than RMB 50,000 but not more than RMB 500,000; where the circumstances are relatively serious, detention of not less than five days but not more than fifteen days shall be imposed, and a fine of not less than RMB 100,000 but not more than RMB 1,000,000 may be imposed concurrently.

Where a unit commits the acts described in the preceding paragraph, the public security organ shall confiscate the illegal gains and impose a fine of not less than RMB 100,000 but not more than RMB 1,000,000, and the persons directly in charge and other directly responsible persons shall be penalized in accordance with the provisions of the preceding paragraph.

Where a person who has violated Article 29 of this Law is subjected to public security administration punishment, he or she shall not hold positions in cybersecurity administration or key network operation positions within five years; where a person is subjected to criminal punishment, he or she shall be permanently prohibited from holding positions in cybersecurity administration or key network operation positions.

Article 67 — Where an operator of critical information infrastructure, in violation of Article 37 of this Law, uses network products or services that have not undergone security review or that have failed security review, the relevant competent department shall order it to make corrections within a prescribed time limit, cease use, and eliminate the impact on national security, impose a fine of not less than one time but not more than ten 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 directly responsible persons.

Article 68 — Where a person, in violation of Article 48 of this Law, sets up websites or communication groups for committing illegal or criminal activities, or uses networks to publish information relating to the commission of illegal or criminal activities, and the act does not constitute a crime, the public security organ shall impose detention of not more than five days, and may concurrently impose a fine of not less than RMB 10,000 but not more than RMB 100,000; where the circumstances are relatively serious, detention of not less than five days but not more than fifteen days shall be imposed, and a fine of not less than RMB 50,000 but not more than RMB 500,000 may be imposed concurrently. Websites and communication groups used for committing illegal or criminal activities shall be closed.

Where a unit commits the acts described in the preceding paragraph, the public security organ shall impose a fine of not less than RMB 100,000 but not more than RMB 500,000, and the persons directly in charge and

other directly responsible persons shall be penalized in accordance with the provisions of the preceding paragraph.

Article 69 — Where a network operator, in violation of Article 49 of this Law, fails to stop transmitting information the publication or transmission of which is prohibited by laws or administrative regulations, take disposal measures such as elimination, preserve relevant records, or report to the relevant competent departments, or, in violation of Article 52 of this Law, fails to stop transmitting information the publication or transmission of which is prohibited by laws or administrative regulations, take disposal measures such as elimination, or preserve relevant records in accordance with the requirements of the relevant departments, the relevant competent department shall order it to make corrections, give it a warning and issue a notice of criticism, and may impose a fine of not less than RMB 50,000 but not more than RMB 500,000; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 500,000 but not more than RMB 2,000,000 shall be imposed, and the relevant competent department may also order suspension of relevant business, suspension of business for rectification, closure of the website or application, revocation of the relevant business license or revocation of the business license, and the persons directly in charge and other directly responsible persons shall be fined not less than RMB 50,000 but not more than RMB 200,000.

Where the acts described in the preceding paragraph cause particularly serious impact or particularly serious consequences, the relevant competent department shall impose a fine of not less than RMB 2,000,000 but not more than RMB 10,000,000, order suspension of relevant business, suspension of business for rectification, closure of the website or application, revocation of the relevant business license or revocation of the business license, and impose a fine of not less than RMB 200,000 but not more than RMB 1,000,000 on the persons directly in charge and other directly responsible persons.

Where providers of electronic information sending services or application software downloading services fail to fulfill the security management obligations prescribed in paragraph 2 of Article 50 of this Law, they shall be penalized in accordance with the provisions of the preceding two paragraphs.

Article 70 — Where a network operator, in violation of this Law, commits any of the following acts, the relevant competent department shall order it to make corrections; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and the persons directly in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000:

(1) refusing or obstructing the supervision and inspection lawfully conducted by the relevant departments; or

(2) refusing to provide technical support and assistance to public security organs and state security organs.

Article 71 — Where any of the following acts is committed, it shall be handled and penalized in accordance with the provisions of the relevant laws and administrative regulations:

(1) publishing or transmitting information the publication or transmission of which is prohibited by paragraph 2 of Article 13 of this Law and other laws and administrative regulations;

(2) infringing upon personal information rights and interests in violation of paragraph 3 of Article 24 and Articles 43 through 45 of this Law; or

(3) in violation of Article 39 of this Law, an operator of critical information infrastructure storing personal information and important data abroad, or providing personal information and important data abroad.

Where a person, in violation of Article 46 of this Law, steals or obtains personal information by other illegal means, or illegally sells or illegally provides personal information to others, and the act does not constitute a crime, the public security organ shall penalize the person in accordance with the provisions of the relevant laws and administrative regulations.

Article 72 — Where a person commits an illegal act prescribed in this Law, it shall be recorded in the credit archives in accordance with the provisions of the relevant laws and administrative regulations, and shall be made public.

Article 73 — Where a person violates this Law but has circumstances of lighter punishment, mitigated punishment or exemption from punishment prescribed in the Administrative Penalty Law of the People's Republic of China, lighter punishment, mitigated punishment or exemption from punishment shall be applied in accordance with the provisions thereof.

Article 74 — Where an operator of a government network of a state organ fails to fulfill the cybersecurity protection obligations prescribed in this Law, its superior organ or the relevant organ shall order it to make corrections; the persons directly in charge and other directly responsible persons shall be given sanctions in accordance with the law.

Article 75 — Where the cyberspace administration department and relevant departments, in violation of Article 32 of this Law, use information obtained in the performance of their cybersecurity protection duties for other purposes, the persons directly in charge and other directly responsible persons shall be given sanctions in accordance with the law.

Where staff of the cyberspace administration department and relevant departments neglect their duties, abuse their powers, or engage in malpractices for personal gain, and the act does not constitute a crime, they shall be given sanctions in accordance with the law.

Article 76 — Where a person violates this Law and causes damage to others, he or she shall bear civil liability in accordance with the law.

Where a violation of this Law constitutes a violation of public security administration, public security administration punishment shall be imposed in accordance with the law; where it constitutes a crime, criminal liability shall be pursued in accordance with the law.

Article 77 — Where institutions, organizations or individuals outside the territory engage in activities endangering the cybersecurity of the People's Republic of China, legal liability shall be pursued in accordance with the law; where serious consequences are caused, the public security department and relevant departments of the State Council may also decide to freeze the property of or take other necessary sanctions against such institutions, organizations or individuals.

Chapter VII — Supplementary Provisions

Article 78 — For the purposes of this Law, the following terms shall have the following meanings:

(1) "Network" means a system composed of computers or other information terminals and related equipment that collects, stores, transmits, exchanges and processes information in accordance with certain rules and procedures.

(2) "Cybersecurity" means the state in which a network operates in a stable and reliable manner, and the capability to ensure the integrity, confidentiality and availability of network data, by taking necessary measures to prevent attacks, intrusions, interference, destruction and illegal use of the network and to prevent accidents.

(3) "Network operator" means the owner and administrator of a network and the network service provider.

(4) "Network data" means all kinds of electronic data collected, stored, transmitted, processed and generated through a network.

(5) "Personal information" means all kinds of information recorded electronically or by other means that can identify the identity of a natural person, alone or in combination with other information, including but not limited to the natural person's name, date of birth, identity document number, personal biometric information,

address, telephone number, and so forth.

Article 79 — In addition to complying with this Law, the security protection of the operation of networks that store and process information involving state secrets shall also comply with the provisions of laws and administrative regulations on the protection of secrets.

Article 80 — The security protection of military networks shall be prescribed separately by the Central Military Commission.

Article 81 — This Law shall come into force on June 1, 2017.

Disclaimer: This English translation is provided for reference and informational purposes only and is an unofficial translation of the Cybersecurity Law of the People's Republic of China. While every effort has been made to ensure accuracy, in the event of any discrepancy between this translation and the original Chinese text, the original Chinese text shall prevail. This translation is not intended as legal advice.