Unofficial translation

CYBERSECURITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA

Source: China Securities Regulatory Commission www.csrc.gov.cn

Chapter 1. General Provisions

Article 1. This Law is formulated for the purposes of protecting 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 shall apply to the construction, operation, maintenance and use of networks as well as the supervision and administration of cybersecurity within the territory of the People's Republic of China.

Article 3. The State attaches equal importance to cybersecurity and the development of information technology and abides by the principles of active use, scientific development, management in accordance with the law, and ensuring security. The State promotes the construction of network infrastructure and interconnectivity, encourages the innovation and application of network technologies, supports the training of qualified cybersecurity personnel, and is committed to establishing a comprehensive cybersecurity system and enhancing cybersecurity capabilities.

Article 4. The State shall formulate and continuously improve cybersecurity strategies, specify the basic requirements and major objectives for ensuring cybersecurity, and propose cybersecurity policies, tasks, and procedures for key sectors.

Article 5. The State shall adopt measures to monitor, prevent and handle cybersecurity risks and threats from both inside and outside the territory of the People's Republic of China. The State shall protect critical information infrastructure against attacks, intrusion, interference and damage, punish unlawful and criminal cyber activities in accordance with the law, and maintain cyberspace security and order.

Article 6. The State shall advocate sincere, honest, healthy and civilized online conduct, advance the dissemination of core socialist values, adopt measures to improve awareness of cybersecurity issues, and create a favorable environment for promoting cybersecurity with the participation of the entire society.

Article 7. The State shall actively engage in international exchanges and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, and attacking cybercrime and illegality. The State shall promote the construction of a peaceful, secure, open and cooperative cyberspace, and establish a multilateral, democratic and transparent network governance system.

Article 8. The national cyberspace authorities shall be responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration tasks. The State Council departments for telecommunications, public security, and other relevant organs shall be responsible for cybersecurity protection, supervision, and management tasks within the scope of their responsibilities, in accordance with the provisions of this Law and other relevant laws and administrative regulations.

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

Article 9. Network operators shall, when conducting business operations and providing services, abide by laws and administrative regulations, respect social morality, observe business ethics, operate in good faith, perform their obligations to safeguard cybersecurity, accept supervision by the government and the public, and undertake social responsibilities.

Article 10. The construction and operation of networks and the provision of network-based services shall be completed in accordance with the provisions of laws and administrative regulations and compulsory national standards. Technical measures and other necessary measures shall be taken in order to ensure cybersecurity and operational stability, provide an effective response to cybersecurity incidents, prevent cybercrimes, and maintain the integrity, confidentiality and availability of online data.

Article 11. Internet-related industry organizations shall, in accordance with their charters, improve industry self-discipline, formulate codes of conduct on cybersecurity, instruct their members to strengthen cybersecurity measures, improve cybersecurity capabilities, and promote the healthy development of the industry.

Article 12. The State shall protect the rights of citizens, legal persons and other organizations to use networks in accordance with the law, promote improved network access, provide better network services, provide the public with secure and convenient network services, and guarantee the lawful, orderly and free circulation of network-based information.

Any individual or organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they shall not endanger cybersecurity or use networks to engage in any activities that endanger national security, national honor and national interests; they shall not incite subversion of national sovereignty or the overthrow of the socialist system, incite separatism or undermine national unity, advocate terrorism or extremism, propagate ethnic hatred or discrimination, disseminate violent or pornographic information, fabricate or disseminate false information to disrupt economic and social order, or infringe upon the reputation, privacy, intellectual property rights or other lawful rights and interests of others.

Article 13. The State shall support the research and development of network products and services that are conducive to the healthy development of minors; the State shall punish the use of networks to engage in activities that endanger the physical and mental health of minors in accordance with the law, and provide a safe and healthy network environment for minors.

Article 14. Any individual or organization shall have the right to report conduct that endangers cybersecurity to the cyberspace authorities, telecommunications authorities, public security authorities, or other relevant authorities. The receiving authority shall handle such reports in a timely manner in accordance with the law, or transfer the report to the competent department in a timely manner if it does not fall within its responsibility.

The relevant department shall keep the informant's information confidential and protect the informant's lawful rights and interests.

Chapter 2. Cybersecurity Support and Promotion

Article 15. The State shall establish and improve a system of cybersecurity standards. The standardization administrative department of the State Council and other relevant departments of the State Council shall, according to their respective functions, organize the formulation of and revise at the appropriate time national and industry standards relating to cybersecurity administration and the security of network products, services, and operations.

The State shall support enterprises, research institutions, higher education institutions, and network-related industry organizations to participate in the formulation of national and industry standards on cybersecurity.

Article 16. The State Council and people's governments of provinces, autonomous regions, and municipalities directly under the Central Government shall conduct overall planning, increase investment, support key cybersecurity technology industries and projects, support the research, development, and application of cybersecurity technologies, promote safe and reliable network products and services, protect the intellectual property rights of network technologies, and support enterprises, research institutions, and higher education institutions in participating in national innovation projects on cybersecurity technologies.

Article 17. The State shall boost the construction of a comprehensive service ecosystem for cybersecurity, and encourage relevant enterprises and institutions to provide cybersecurity certifications, testing, risk assessment, and other security services.

Article 18. The State shall encourage the development of technologies for protecting and using network data, promote the availability of public data assets, and promote technological innovation and social and economic development.

The State shall support innovation in cybersecurity administration and encourage the application of new network technologies to enhance cybersecurity.

Article 19. People's governments at all levels and their relevant departments shall organize regular cybersecurity publicity events and education campaigns, and instruct and encourage relevant entities to conduct effective cybersecurity publicity and education campaigns.

The mass media shall conduct targeted cybersecurity publicity and education campaigns aimed at the public.

Article 20. The State shall provide support to enterprises, higher education institutions, vocational schools, and other education training institutions to conduct cybersecurity-related education and training activities, employ a range of methods to train qualified cybersecurity personnel, and promote exchanges between cybersecurity professionals.

Chapter 3. Network Operations Security

Section 1. General Provisions

Article 21. The State shall implement a multi-level cybersecurity protection system. Network operators shall perform the following security protection duties according to the requirements of the multi-level

cybersecurity protection system to ensure that networks are free from interference, damage or unauthorized access, and prevent network data from being disclosed, stolen or falsified:

(i) Formulate internal security administration rules and operating procedures, determine the persons in charge of cybersecurity, and carry out their cybersecurity responsibilities;

(ii) Adopt technical measures to prevent computer viruses, cyber attacks, network intrusions, and other activities which may endanger cybersecurity;

(iii) Adopt technical measures to monitor and record the status of network operations and cybersecurity incidents, and store relevant network logs for at least six months in accordance with regulations;

(iv) Adopt measures such as data classification, backup of important data, and data encryption;

(v) Other obligations as prescribed by laws and administrative regulations.

Article 22. Network products and services shall comply with the mandatory requirements of relevant national standards. Providers of network products and services shall not install malware. When a provider discovers a security flaw or vulnerability in its network products or services, it shall immediately take remedial measures and follow provisions to promptly inform users and report the incident to the competent department.

Providers of network products and services shall provide security maintenance services for their products and services, and shall not terminate the provision of security maintenance services during the stipulated period or the period agreed between the relevant parties.

If a network product or service collects user information, the provider shall clearly indicate this and obtain consent from the user. If a user's personal information is involved, the provider shall also comply with the provisions of this law and the provisions of relevant laws and administrative regulations on the protection of personal information.

Article 23. Critical network equipment and specialized cybersecurity products shall, in accordance with the mandatory requirements of relevant national standards, be certified by a qualified institution or meet the requirements of a security inspection prior to being sold or provided. The national cyberspace authorities shall, in conjunction with relevant departments of the State Council, develop and release a catalog of critical network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security inspection results to avoid repeated certifications and inspections.

Article 24. Network operators who provide network access and domain registration services for users, process network access formalities for fixed-line or mobile phone users, or provide users with information publication services or instant messaging services shall require users to provide details of their identity when signing agreements with users or confirming the provision of services. If a user fail to provide his or her identify details, the network operator shall not provide the user with relevant services.

The State shall implement a strategy of trusted identities in cyberspace, support the research and development of secure and convenient electronic identity authentication technologies, and promote mutual recognition among different electronic identity authentication methods.

Article 25. Network operators shall formulate emergency response plans for cybersecurity incidents and address system vulnerabilities, computer viruses, cyber attacks, network intrusions, and other security risks in a timely manner. When a cybersecurity incident occurs, the relevant operator shall immediately initiate the emergency response plan, adopt corresponding remedial measures, and report the incident to the competent authorities in accordance with relevant provisions.

Article 26. Cybersecurity certification, testing, risk assessment, or other such activities, and the publication of cybersecurity information such as system vulnerabilities, computer viruses, network attacks, or network intrusions shall comply with relevant national provisions.

Article 27. No individual or organization may engage in any activity

which endangers cybersecurity, such as illegally intruding into another person's network, interfering with the normal functions of another person's network, stealing network data, or providing programs or tools specifically used for conducting activities that endanger cybersecurity, such as network intrusion, interference with normal network functions and protection measures, and the stealing of network data. Where someone is aware that another person is engaging in actions that endanger cybersecurity, he/shall shall not provide assistance such as technical support, advertisements or promotions, or payment of expenses.

Article 28. Network operators shall provide technical support and assistance to public security bodies and national security bodies acting to maintain national security and investigate criminal activities.

Article 29. In order to enhance the cybersecurity capabilities of network operators, the State supports cooperation between network operators in areas such as the gathering, analysis, reporting, and emergency handling of cybersecurity information.

Relevant industry organizations shall formulate comprehensive cybersecurity standards and coordination mechanisms for their respective industry, strengthen their analysis and evaluation of cybersecurity matters, and periodically provide members with risk alerts, support, and assistance in responding to cybersecurity risks.

Article 30. Information obtained by the cyberspace authorities and other relevant departments during the performance of cybersecurity protection duties may only be used for cybersecurity needs, and may not be used for other purposes.

Section 2. Operations Security For Critical Information Infrastructure

Article 31. In addition to the multi-level cybersecurity protection system, the State shall implement protection measures for public communication and information services, energy, transportation, water resources, finance, public

services, e-government services, and other critical information infrastructure which may gravely endanger national security, people's livelihoods, or the public interest if such infrastructure is destroyed, loses its function, or experiences data leaks. The specific scope of critical information infrastructure and relevant security measures shall be formulated by the State Council.

The State encourages network operators who do not use critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

Article 32. In accordance with the division of responsibilities provided by the State Council, departments responsible for the protection of critical information infrastructure shall formulate and organize the implementation of security plans for their industry's critical information infrastructure, and guide and supervise efforts to protect the security of critical information infrastructure.

Article 33. Organization that construct critical information infrastructure shall ensure that it can provide a stable and continuous service, and guarantee that technical security measures are planned, established, and used concurrently.

Article 34. In addition to the provisions of Article 21 of this Law, operators of critical information infrastructure shall perform the following security obligations:

(i) Set up specialized security management institutions and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;

(ii) Conduct periodic cybersecurity education, technical training, and skills assessments for employees;

(iii) Conduct disaster recovery backups of important systems and databases;

(iv) Formulate emergency response plans for cybersecurity incidents, and organize periodic drills;

(v) Other obligations as prescribed by laws and administrative regulations.

Article 35. Operators of critical information infrastructure who purchase network products and services that may influence national security shall undergo a security review organized by the national cyberspace authorities and relevant departments of the State Council.

Article 36. Operators of critical information infrastructure who purchase network products and services shall follow the relevant provisions and sign a security and confidentiality agreement with the provider which clarifies the operator's security and confidentiality obligations and responsibilities.

Article 37. Operators of critical information infrastructure that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China shall store such information/data within Mainland China. If, due to business requirements, it is necessary provide such information/data outside of the territory of Mainland China, a security assessment shall be conducted according to the measures jointly formulated by the national cyberspace authorities and relevant departments of the State Council. Where laws or administrative regulations provide otherwise, those provisions shall apply.

Article 38. At least once per year, operators of critical information infrastructure shall conduct an assessment of potential network security risks, either personally or by entrusting a cybersecurity services provider. The results of this assessment and improvement measures should be submitted to the relevant department responsible for the security of critical information infrastructure.

Article 39. The national cyberspace authorities shall assist the relevant authorities in employing the following measures for protecting the security of critical information infrastructure:

(i) Conduct random tests of security risks to critical information infrastructure, propose measures for improvement, and where necessary entrust a cybersecurity services provider to conduct testing and assessment of cybersecurity risks.

(ii) Organize periodic emergency cybersecurity drills for operators of critical information infrastructure in order to increase their ability to respond to cybersecurity incidents;

(iii) Promote sharing of cybersecurity information among relevant departments, operators of critical information infrastructure, relevant research institutions and cybersecurity services providers;

(iv) Provide technical support and assistance for cybersecurity incident response and network function recovery.

Chapter 4. Network Information Security

Article 40. Network operators shall strictly maintain the confidentiality of any user information collected, and establish a comprehensive system for protecting user information.

Article 41. Network operators who collect and use personal information shall abide by the principles of legality, propriety, and necessity; they shall disclose the rules for collecting and using such information, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the users whose data is being collected.

Network operators shall not collect personal information which is unrelated to the services they provide or collect or use personal information in violation of the provisions of laws, administrative regulations, or user agreements. Network operators shall follow the provisions of laws, administrative regulations, and user agreements when processing personal information.

Article 42. Network operators shall not disclose, tamper with, or damage personal information; personal information may not be provided to others without the agreement of the user whose information is being collected, except where it has been processed in such a manner that it is impossible to identify a particular individual and the information cannot be recovered.

Network operators shall adopt technical and other necessary measures to ensure the security of personal information they collect and to prevent personal information from being disclosed, damaged or lost. In the event of such disclosure, damage or loss, remedial measures shall be promptly taken and users shall be notified in a timely manner, and the matter shall be reported to the competent department in accordance with regulations.

Article 43. If an individual discovers that a network operator has violated the provisions of laws, administrative regulations or user agreements in collecting or using his/her personal information, he/she has the right to request the network operator to delete his/her personal information. If the personal information collected or retained by the network operator contains errors, he/she has the right to request the network operator to correct such errors. In these circumstances, network operators shall adopt measures to delete or correct such data.

Article 44. Individuals or organizations must not steal or use other illegal means to acquire personal information, and must not unlawfully sell or unlawfully provide others with personal information.

Article 45. Departments and their personnel who are responsible for cybersecurity supervision and administration must keep personal information, private information, and trade secrets obtained during the performance of their duties strictly confidential, and shall not disclose, sell, or unlawfully provide such information to others.

Article 46. All individuals and organizations shall be responsible for the activities that they conduct when using networks and must not establish websites or communication groups in order to commit fraud, disseminate criminal activities, produce or sell prohibited or controlled goods, or engage in other unlawful and criminal activities. Networks must not be used to publish information related to fraud, the production or sale of prohibited or controlled goods, or other unlawful activities.

Article 47. Network operators shall improve the management of information published by users, and upon discovering information of which the publication or dissemination is prohibited by laws and regulations, they

shall immediately stop the dissemination of such information and adopt measures such as deleting the information, preventing the information from spreading, and retaining relevant records, and report the incident to the competent authority.

Article 48. Electronic information sent or application software provided by any individual or organization shall not install malware or contain information that is prohibited from being published or transmitted by laws and administrative regulations.

Providers of electronic information distribution services and application software download services shall perform their security obligations; where they know that their users have engaged in conduct listed in the preceding paragraph, they shall adopt appropriate measures such as suspending the provision of services, deleting information and retaining relevant records, and report the incident to the competent authority.

Article 49. Network operators shall establish a complaints and reporting system for issues related to network security, publish the methods for making complaints or reports, and promptly accept and handle complaints and reports related to network security.

Network operators shall cooperate with the cyberspace authorities and relevant departments in conducting monitoring procedures and investigations in accordance with the law.

Article 50. The national cyberspace authorities and relevant departments shall be responsible for monitoring and managing the security of online content. Where they discover the publication or transmission of information which is prohibited by laws or administrative regulations, they shall request that network operators stop the transmission of such information and employ removal measures such as deletion, as well as retain relevant records; for information described above that comes from outside of the territory of the People's Republic of China, they shall notify the relevant organization to adopt technical measures and other necessary measures to block the transmission of such information.

Chapter 5. Monitoring, Early Warning and Emergency Response

Article 51. The State shall establish a cybersecurity monitoring, early warning and information reporting system. The national cyberspace authorities shall coordinate with relevant authorities to improve the collection, analysis, and reporting of cybersecurity information, and publish cybersecurity monitoring and advance warning information in accordance with regulations.

Article 52. Departments responsible for the security and protection of critical information infrastructure shall establish robust cybersecurity monitoring, early warning and information reporting systems for their respective industries or sectors, and shall report cybersecurity monitoring and early warning information in accordance with regulations.

Article 53. The national cyberspace authorities shall coordinate with relevant departments to establish comprehensive cybersecurity risk assessment and emergency response mechanisms, formulate emergency plans for cybersecurity incidents, and organize periodic drills.

Departments responsible for the security and protection of critical information infrastructure shall formulate cybersecurity incident response plans for their respective industries and sectors, and organize periodic drills.

In the event of a cybersecurity incident, the cybersecurity incident response plan shall grade the incident according to the degree of harm caused and scope of its impact, and stipulate the corresponding emergency response measures.

Article 54. When the risk of a cybersecurity incident increases, the relevant departments of the people's governments at or above the provincial level shall, in accordance with the prescribed authority and procedures, adopt the following measures according to the characteristics of the cybersecurity risk and its potential harm:

(i) Require relevant departments, institutions, and personnel to collect and report relevant information in a timely manner, and strengthen monitoring of cybersecurity risks;

(ii) Organize relevant departments, institutions, and specialist personnel to analyze and assess information on the cybersecurity risk, and predict the likelihood of occurrence, the scope of impact, and the degree of harm were such incident to occur;

(iii) Issue cybersecurity warnings to the public, and publish measures to mitigate harm.

Article 55. When a cybersecurity incident occurs, the cybersecurity incident response plan shall be initiated immediately, and the incident shall be investigated and assessed. Network operators shall adopt technical measures and other necessary measures to eliminate hidden security threats and prevent the spread of harm, and must promptly issue warnings which are relevant to the public.

Article 56. While performing cybersecurity supervision and management duties, if relevant departments of people's governments at the provincial level or above discover that there is a significant security risk on a particular network, or if a security incident occurs, such departments may require the legal representative or manager of the network operator to attend an interview in accordance with stipulated procedures and the department's scope of authority. Network operators shall adopt measures in accordance with requirements and take remedial action in order to eliminate hidden threats.

Article 57. If an emergency or occupational accident occurs as a result of a cybersecurity incident, it shall be dealt with in accordance with the provisions of the Emergency Response Law of the People's Republic of China, Work Safety Law of the People's Republic of China, and other laws and administrative regulations.

Article 58. Due to the need to protect national security, maintain public order, and respond to major security incidents, temporary measures such as restrictions on network communications may be imposed in particular regions as determined or approved by the State Council.

Chapter 6. Legal Responsibility

Article 59. If a network operator fails to perform its cybersecurity obligations as stipulated in Articles 21 and 25 of this Law, the relevant competent department shall order the network operator to take corrective action and issue a warning; if the network operator refuses to take corrective action, endangers cybersecurity or causes other consequences, a fine of RMB10,000 to RMB100,000 shall be levied, and the supervisor directly responsible shall be subject to a fine of RMB5,000 to RMB50,000.

Where an operator of critical information infrastructure fails to perform its cybersecurity obligations as stipulated in Articles 33, 34, 36, and 38 of this Law, the relevant competent department shall order the network operator to take corrective action and issue a warning; if the network operator refuses to take corrective action, endangers cybersecurity or causes other consequences, a fine of RMB100,000 to RMB1,000,000 shall be imposed, and the directly responsible supervisor shall be subject to a fine of RMB10,000 to RMB100,000.

Article 60. Where the provisions of Articles 22.1, 22.2 and 48.1 of this Law are violated by any of the following conduct, the relevant competent department shall order the offender to take corrective action and issue a warning; if the offender refuses to take corrective action, endangers cybersecurity or causes other consequences, a fine of RMB50,000 to RMB100,000 shall be levied, and the directly responsible supervisor shall be subject to a fine of RMB10,000 to RMB100,000:

(i) Installation of malware;

(ii) Failure to adopt immediate remedial measures for security flaws or vulnerabilities in products and services, or not informing users and reporting to the competent authorities in accordance with regulations;

(iii) Unauthorized termination of security maintenance measures for products and services.

Article 61. If a network operator fails to require users to provide details of

their identity, or provides services to users who have not provided details of their identity in violation of the provisions of Article 24.1 of this Law, the relevant competent department shall order the network operator to take corrective action; if the network operator refuses to take corrective action or in the event of a serious violation, a fine of RMB50,000 to RMB500,000 shall be levied, and the relevant competent department may order the network operator to temporarily suspend operations, take down its website, or revoke its business permits or business licenses; the directly responsible supervisor or other directly responsible personnel shall be subject to a fine of RMB10,000 to RMB100,000.

Article 62. If activities such as cybersecurity certification, testing, or risk assessments are conducted, or information on system vulnerabilities, computer viruses, cyber attacks, and network intrusions is released to the public in violation of the provisions of Article 26 of this Law, the relevant competent department shall order the offender to take corrective action and issue a warning; if the offender refuses to take corrective action or in the event of a serious violation, a fine of RMB10,000 to RMB100,000 shall be levied, and the relevant competent department may order the offender to temporarily suspend operations, take down its website, or revoke its business permits or business licenses; the directly responsible supervisor or other directly responsible personnel shall be subject to a fine of RMB5,000 to RMB50,000.

Article 63. In the event that Article 27 of this Law is violated due to engagement in activities which endanger cybersecurity, the provision of programs, tools, or services that are specifically used for conducting activities which endanger cybersecurity, or the provision of technical support, advertising, payment of expenses, or other assistance, if the violation does not constitute a crime, the public security authorities shall confiscate any illegal income, detain the offenders for a maximum of five days, and levy a fine of RMB50,000 to RMB500,000; in serious circumstances, the public security authorities shall detain the offenders for a period of 5 to 15 days and levy a fine of RMB100,000 to RMB1,000,000.

If an organization engages in conduct listed in the preceding paragraph,

the public security authorities shall confiscate any illegal income, levy a fine of RMB100,000 to RMB1,000,000, and punish the directly responsible supervisor and other directly responsible personnel in accordance with the provisions of the preceding paragraph.

Where Article 27 of this Law is violated, persons who receive public security administrative sanctions must not engage in cybersecurity management or work in key network operations positions for 5 years; persons who receive criminal sentences will be subject to a lifetime ban on working in cybersecurity management and key network operations positions.

Article 64. Network operators and network product or service providers who violate Article 22.3 or Articles 41-43 of this Law by infringing on personal information that is protected in accordance with law shall be ordered to take corrective action by the relevant competent authorities and may, either independently or concurrently, be given warnings, be subject to confiscation of unlawful gains, and/or be fined between 1 to 10 times the amount of any unlawful gains; where there are no unlawful gains, the fine shall be up to RMB 1,000,000, and a fine of between RMB 10,000 and 100,000 shall be levied on persons who are directly in charge and other directly responsible personnel; in the event of a serious violation, the relevant competent department may order the offender to temporarily suspend operations, close down the offender's website, or revoke the offender's operational permits or business licenses.

Where Article 44 of this Law is violated due to the stealing of personal information or use of other illegal means to obtain, illegally sell, or illegally provide others with personal information, and this does not constitute a crime, the public security authorities shall confiscate unlawful gains and levy a fine of between 1 and 10 times the amount of unlawful gains; where there are no unlawful gains, the public security authorities shall levy a fine of up to RMB 1,000,000.

Article 65. Where operators of critical information infrastructure violate Article 35 of this Law by using network products or services that have failed or not completed a security inspection, the relevant competent department shall order the operator to suspend the use of such products and levy a fine

of 1 to 10 times the purchase price; the directly responsible supervisor and other directly responsible personnel shall be subject to a fine of RMB10,000 to RMB100,000.

Article 66. Where an operator of critical information infrastructure violates Article 37 of this Law by storing network data overseas or providing network data overseas, the relevant competent department shall order the operator to take corrective action, issue a warning, confiscate any illegal income, levy a fine of RMB50,000 to RMB100,000, and may order the operator to temporarily suspend operations, take down the operator's websites, or revoke the operator's business permits or licenses; the directly responsible supervisor and other directly responsible personnel shall be subject to a fine of RMB10,000 to RMB100,000.

Article 67. Where Article 46 of this Law is violated by establishing a website or communications group used for conducting illegal or criminal activities, or a network is used to publish information on conducting illegal or criminal activities, the public security authorities shall detain the offenders for up to five days, and may levy a fine RMB10,000 to RMB100,000; in serious circumstances, the offender shall be detained for five days to 15 days and may be subject to a fine of RMB50,000 to RMB500,000. The public security authorities may also close down websites and communications groups used for illegal or criminal activities.

If an organization engages in any of the conduct listed in the preceding Paragraph, the public security authorities shall impose a fine of RMB100,000 to RMB500,000 and fine the directly responsible supervisor and other directly responsible personnel in accordance with the provisions of the preceding Paragraph.

Article 68. If a network operator violates Article 47 of this Law by failing to stop the transmission of information which is prohibited from being published or transmitted by laws or administrative regulations, failing to employ disposition measures such as deletion, or failing to retain relevant records, the relevant competent department shall order the operator to take corrective action, issue a warning, and confiscate any illegal income. If corrective action is refused or in serious circumstances, a fine of RMB100,000

to RMB500,000 shall be levied and the operator may be ordered to temporarily suspend business, take down its website, or the operator's business permits or licenses may be revoked; the directly responsible supervisor and other directly responsible personnel shall be subject to a fine of RMB10,000 to RMB100,000.

Where providers of electronic information transmission services or application software download services fail to perform their security obligations provided for in Article 48.2 of this Law, they shall be punished in accordance with the provisions of the preceding Paragraph.

Article 69. Network operators who violate the provisions of this Law by engaging in any of the following conduct shall be ordered to take corrective action by the relevant competent authority; if the network operator refuses to take correct action or in serious circumstances, a fine of RMB50,000 to RMB500,000 shall be levied, and the directly responsible supervisor and other directly responsible personnel shall be subject to a fine of RMB10,000 to RMB100,000:

(i) Failure to comply with the requirements of relevant departments to take measures to stop the transmission of or delete information of which the publication or dissemination is prohibited by laws and administrative regulations;

(ii) Refusing or obstructing the supervisions and inspections carried out by authorities in accordance with law;

(iii) Refusal to provide technical support and assistance to public security authorities and State security authorities.

Article 70. The publication or transmission of information prohibited by Article 12.2 of this Law or other laws or administrative regulations shall be punished in accordance with the provisions of relevant laws and administrative regulations.

Article 71. Actions which violate the provisions of this Law shall be recorded in the credit file of the offender and made public in accordance with the provisions of relevant laws and administrative regulations.

Article 72. Where the operator of a State authority's government affairs network fails to perform its cybersecurity protection obligations as provided in this Law, its superior authority or relevant authority shall order it to take corrective action; the directly responsible supervisor and other directly responsible personnel shall be punished in accordance with the law.

Article 73. Where the cyberspace authorities and other relevant authorities violate the provisions of Article 30 of this Law by using personal information acquired while performing cybersecurity obligations for other purposes, the directly responsible supervisor and other directly responsible personnel shall be punished in accordance with the law.

In the event that personnel of cyberspace authorities and other relevant authorities neglect their duties, abuse their authority, or engage in bribery and fraud, and such actions do not constitute a crime, such personnel shall be punished in accordance with the law.

Article 74. Those who violate the provisions of this Law and cause harm to others shall bear civil liability in accordance with law.

If any provisions of this Law are violated, constituting a violation of public order management, public order administrative sanctions will be imposed in accordance with the law; if it constitutes a crime, offenders shall be investigated for criminal liability in accordance with law.

Article 75. Where an overseas institution, organization, or individual engages in attacks, intrusions, interference, damage, or other activities that endanger the critical information infrastructure of the People's Republic of China, resulting in significant consequences, the institution, organization, or individual shall be investigated for legal liability in accordance with the law; the public security authorities of the State Council and other relevant departments may decide to freeze the assets of such institution, organization, or individual or impose other necessary sanctions.

Chapter 7. Miscellaneous

Article 76. The definitions of terms used in this Law are as follows:

(i) "Network" refers to a system consisting of computers or other information terminals and related equipment that collects, retains, transmits, exchanges, and processes information according to certain rules and procedures.

(ii) "Cybersecurity" refers to the ability to prevent network attacks, intrusions, interference, damage, illegal use, and accidents, to make networks stable and reliable, and to ensure the integrity, confidentiality, and availability of network data.

(iii) "Network operator" refers to network owners, administrators, and network service providers.

(iv) "Network data" refers to all kinds of electronic data collected, stored, transmitted, processed, and generated through networks.

(v) "Personal information" refers to information recorded electronically or through other means that can identify a natural person's personal identity, either on its own or in combination with other information, including but not limited to a natural person's name, date of birth, ID number, personal biometric information, address, and telephone number.

Article 77. The operation and security of networks that retain and process State secrets shall, in addition to complying with this Law, comply with the provisions of laws and administrative regulations pertaining to secrecy protection.

Article 78. The security protection rules for military networks shall be formulated by the Central Military Commission.

Article 79. This Law is implemented as of June 1, 2017.

This translation is provided for reference purposes only and without any warranty or representation regarding its accuracy or completeness. Reliance on this translation is at your own risk. If you would like to report a translation error or inaccuracy, we encourage you to please contact us.