The Cryptography Law of the People's Republic of China (October 26, 2019, the ninth and third session of the National People's Representative Conference, the fourth meeting of the Standing Committee Negotiated)

October 27, 2019 14:52 Source: Chinese People's [redacted] 【print】【Error correction】

Cryptography Law of the People's Republic of China

(Adopted at the fourth meeting of the Standing Committee of the Third and Third National People's Congress on October 26, 2019)

◆ Record

Chapter 1 General Provisions

Article 1 In order to standardize the application and management of passwords, promote the development of the cryptographic business, ensure network and information security, maintain national security and social public interests, and protect citizens, law and other organizations' The law is enacted for legitimate rights and interests.

Article 2 The term "password" as used in this law refers to the technologies, products and services that use specific transformation methods to encrypt and protect information, etc., and securely authenticate.

Article 3 " Encryption work adheres to the overall national security concept, and follows the principles of unified leadership, hierarchical responsibility, innovative development, service to the bureau, management in accordance with the law, and security.

Article 4 Uphold the leadership of the Chinese Communist Party in cryptography. The Central Encryption Work Leading Agency implements the unified leadership of the national encryption work, formulates the national encryption work re-targeting policy, and coordinates the coordination Adjust national cryptographic issues and important work, and promote the establishment of the national cryptographic rule of law.

Article State Encryption Management is responsible for the administrative password for the country to work surely. The password management departments at the county level and above are responsible for the management of password operations in their own administrative areas.

State agencies and units involved in cryptography are responsible for the cryptography of their agencies, units, or systems within the scope of their duties.

Article 6: The state implements classified management of passwords.

Passwords are divided into verification passwords, ordinary passwords and commercial passwords.

Article 7: Verification passwords and ordinary passwords are used to protect state secret information. The highest level of verification password-protected information is top-secret level, and the highest level of ordinary password-protected information is confidential level.

Verification passwords and common passwords are state secrets. The password management department implements strict and unified management of verification passwords and ordinary passwords in accordance with this law, relevant laws, administrative regulations, and relevant state regulations.

Article 1 Commercial passwords are used to protect information that is not a state secret.

Citizens, French and other organizations can use commercial passwords to protect network and information security in accordance with the law.

Article 9: The state encourages and supports the research and application of cryptographic science and technology, protects intellectual property rights in the cryptographic field in accordance with the law, and promotes the progress and innovation of cryptographic science and technology.

The state strengthens the training of cryptographic talents and team building, and commends and rewards organizations and individuals that have made outstanding contributions in cryptographic work in accordance with relevant state regulations.

Article 10 The state adopts various forms to strengthen password security education, incorporates password security education into the national education system and the education and training system of civil servants, and strengthens the passwords of citizens, law and other organizations safety consciousness.

Article One: People's governments at or above the county level shall incorporate the password into the national economic and social development plan at the same level, and the required funds shall be listed in the fiscal budget of the same level.

Article 2 Any organization or individual shall not steal other encrypted information or illegally invade other's password protection system.

No organization or individual may use passwords to engage in illegal and criminal activities that endanger national security, social public interests, and other legitimate rights and interests.

Chapter 2 Verification Password, Common Password

Article Three: The state strengthens the scientific planning, management and use of nuclear passwords and ordinary passwords, strengthens system construction, improves management measures, and enhances password security capabilities.

Article 4 State secret information transmitted in wired and wireless communications, as well as information systems that store and process state secret information, shall be used in accordance with laws, political regulations, and relevant state regulations. Use verification passwords and ordinary passwords for encryption protection and security authentication.

Article 5 Institutions (hereinafter collectively referred to as cryptographic agencies) that engage in cryptographic verification, common cryptographic research, production, services, testing, equipment, use, and destruction (hereinafter collectively referred to as cryptographic agencies) shall comply with laws and policies. Regulations, relevant national regulations, and standards for verification of passwords and common passwords, establish a sound security management system, and adopt strict confidentiality measures and confidentiality responsibility systems to ensure verification of passwords and common passwords Security.

Article 6: The password management department shall guide, supervise and inspect the verification passwords and ordinary passwords of the password-making organization in accordance with the law, and the password-making organization shall cooperate.

Article VII: The password management department shall work with relevant departments to establish verification passwords, security monitoring and early warning of ordinary passwords, security risk assessment, information notification, important matters consultations and responses based on operational needs. Collaboration mechanisms such as emergency handling ensure the coordinated linkage and orderly efficiency of the verification password and common password security management.

If the cryptography agency discovers that the verification password or common password is leaked, or there are major problems or hidden risks that affect the security of the verification password or common password, it shall take immediate countermeasures and promptly report to the security authorities. The secret government management department and password management department report, the secret government management department and the password management department will organize investigations and disposals in conjunction with the relevant departments, and guide the relevant password management organizations to eliminate them in time Security risks.

Article 10: The state strengthens the construction of cryptography institutions to ensure that they perform their duties.

The state establishes management systems for the recruitment, selection, confidentiality, assessment, training, treatment, rewards and punishments, exchanges, and withdrawal of personnel that meet the needs of verifying passwords and ordinary passwords.

Article 9 Due to operational needs and in accordance with relevant national regulations, the password management department may ask the public security, transportation, customs and other departments to verify passwords, common password-related items, and provide personnel For convenience such as exemption from inspection, relevant departments shall provide assistance.

Article 2 The password management department and the password production organization shall establish a sound and strict supervision and security review system, supervise their staff's compliance with laws and disciplines, and adopt them in accordance with the law. Take necessary measures to organize and carry out safety reviews on a regular or irregular basis.

Chapter 3 Commercial Password

Article 2 The state encourages the research and development, academic exchanges, achievement transformation, and application of commercial cryptographic technology, completes a unified, open, competitive, and orderly commercial cryptographic market system, and encourages And promote the development of the commercial crypto industry.

People's governments at all levels and their relevant departments should follow the principle of non-discrimination and treat all commercial cryptographic research, production, sales, service, import and export entities, including foreign-invested enterprises, on an equal basis in accordance with the law. (Hereinafter collectively referred to as business cryptography business units). The state encourages the development of commercial cryptographic technology cooperation based on voluntary principles and business rules in the process of foreign investment. Political agencies and their staff shall not make use of the government Mandatory transfer of commercial cryptographic technology.

The scientific research, production, sales, service, import and export of commercial passwords must not harm national security, social public interests, or other legitimate rights and interests.

Article 2 The state establishes and perfects a standard system of commercial passwords.

The State Council's standardization administrative department and the national password management department organize the formulation of national and business standards for commercial passwords in accordance with their respective responsibilities.

The state supports social organizations and enterprises to use their own innovative technologies to formulate commercial cryptographic group standards and corporate standards that are higher than the technical requirements of national standards and business standards.

Article 2 Three The state promotes participation in the international standardization of commercial ciphers, participates in the formulation of international standards for commercial ciphers, and promotes the conversion and application of commercial ciphers between Chinese standards and foreign standards.

The state encourages enterprises, social organizations and educational and scientific research institutions to participate in the international standardization of commercial passwords.

Article 2 Commercial cryptography practitioners carrying out commercial cryptographic activities shall comply with relevant laws, administrative regulations, compulsory national standards for commercial cryptography, and the technical standards disclosed by the business cryptography company Claim.

The state encourages business password practitioners to adopt the recommended national standards and industry standards for business passwords to improve the protection of business passwords and safeguard the legitimate rights and interests of users.

Article Two Five The state promotes the construction of a commercial password testing and certification system, formulates technical specifications and rules for commercial password testing and certification, and encourages business password practitioners to voluntarily accept commercial password testing and certification Certification and enhance market competition.

Commercial password testing and certification agencies shall obtain relevant qualifications in accordance with the law, and carry out commercial password testing and certification in accordance with the provisions of laws, political regulations and technical specifications and rules for commercial password testing and certification.

Commercial password testing and certification agencies shall bear the obligation to keep confidential the state secrets and commercial secrets they know about in the testing and certification of commercial passwords.

Article 8: Article 6 ：Commercial cryptographic products involving national security, national economy and civil affairs, and social and public interests shall be listed in the list of key network equipment and special network security products in accordance with the law. After the agency has passed the inspection and certification, it can be sold or provided. The testing and certification of commercial cryptographic products applies the relevant provisions of the "Network Security Law of the People's Republic of China" to avoid repeated testing and certification.

Commercial cryptographic services that use key network equipment and dedicated products for network security shall be certified by a commercial cryptographic certification agency to qualify for the commercial cryptographic service.

Seventh Article Laws, political regulations, and relevant national regulations require the use of commercial passwords to protect critical information infrastructure, and its operators shall use commercial passwords to protect key information infrastructure. The author entrusts a commercial password testing agency to carry out a security assessment of the application of commercial passwords. The application security assessment of commercial passwords should be consistent with the critical information infrastructure security testing and assessment, and the network security level assessment system Connect with each other to avoid repeated assessments and evaluations.

Critical information infrastructure operators who purchase network products and services involving commercial passwords that may affect national security shall comply with the provisions of the "Network Security Law of the People's Republic of China". It has passed the national security review organized by the State Information Department in conjunction with the State Password Management Department and other relevant departments.

Article 2 The competent commerce department **of the** State Council and the national password management department shall implement licenses for commercial passwords that involve national security, social and public interests and have encryption protection functions in accordance with the law. Commercial ciphers that involve national security, social public interest, or China's international obligations are regulated. The entry of commercial passwords into the permission list and the exit control list are jointly conducted by the competent commercial department of the State Council It is formulated and announced by the National Encryption Administration Department and the General Administration of Customs.

Commercial passwords used by a large number of consumer products are inaccurate in the entry permit and exit control system.

Article 9: The national password management department recognizes institutions that use commercial password technology to engage in e-government and e-authentication services, and is responsible for the use of e-signatures in government activities in conjunction with relevant departments Name and data management.

Article 2: Organizations such as business associations in the field of commercial cryptography provide information, technology, training and other services for commercial cryptography companies in accordance with the provisions of laws, political regulations and their articles of association, guide and Supervise and urge commercial cryptography companies to carry out commercial cryptography activities in accordance with the law, strengthen self-discipline in the business, promote the construction of business integrity, and promote the healthy development of the business.

Article 3 The password management department and relevant departments establish a commercial password interim and ex post supervision system that combines daily supervision and random inspections, and establish a unified commercial password supervision and management information platform. Taiwan, promote the integration of interim and ex-post supervision with the social credit system, and strengthen the self-discipline and social supervision of commercial cryptography business units.

Password management departments and relevant departments and their staff shall not require commercial password practitioners and commercial password testing and certification agencies to disclose source code and other proprietary information related to passwords, The business secrets and personal privacy learned in the performance of duties are kept strictly confidential, and shall not be disclosed or provided to others in violation of the law.

Chapter IV Legal Liability

Article 3 Violating the provisions **of Article 2** of this law, stealing encrypted information protected by others, infringing on another's password protection system without the law, or using passwords to endanger national security and social public For illegal activities such as interests, legal rights and interests of others, the relevant departments shall be investigated for legal responsibility in accordance with the "Network Security Law of the People's Republic of China" and other relevant laws and administrative regulations.

十 three third violation of provisions of Article 24 stipulates 十 not Use Nuclear Center Weighted password, common passwords as required by the password management department shall order correction or stop the illegal 行 was given a warning; plot In serious cases, the password management department recommends that relevant state agencies and units impose sanctions or treatment on the directly responsible personnel in charge and other directly responsible personnel in accordance with the law.

Article 34 In violation of the provisions of this law, a case of verifying passwords or common password leaks is issued, the confidentiality administrative department and the password management department suggest that relevant state agencies and units be directly responsible The supervisors and other directly responsible personnel shall be punished or dealt with in accordance with the law.

Violating the provisions of Article 8.7, Subparagraph 2 of this Law, discovering that the verification password or common password has been leaked, or affecting the verification password and common password security serious problems, risk hazards, and immediately taking countermeasures If it is implemented, or if it fails to report in a timely manner, the confidentiality administrative department and the password management department recommend that relevant state agencies and units impose sanctions or punishments on the directly responsible supervisors and other directly responsible personnel in accordance with the law. 否Handle.

Article 35 Commercial password testing and certification agencies that violate the provisions of Article 8.5, Subparagraph 2 and Paragraph 3 of this law to carry out commercial password testing and certification shall be managed by the market supervision and management department in conjunction with the password management Departments order corrections or suspension of illegal actions, give warnings, and confiscate illegal gains; if the illegal gains are more than 30,000 yuan, a fine of one to three times the illegal gains may be imposed; there is no illegal gains Or if the illegal income is less than 30,000 yuan, a fine of more than 10,000 yuan and less than 30,000 yuan may be imposed concurrently; if the circumstances are serious, the relevant qualifications shall be revoked in accordance with the law.

The third 十 **six** violate second shot 十 26 hereof, sell or offer without testing and certification testing and certification or unqualified providers Using encryption products, or provide certification or certification without fail For commercial password services, the market supervision and management department, together with the password management department, shall order to correct or stop illegal activities, give warnings, and confiscate illegal products and illegal income; illegal income is more than 10,000 yuan If there is no illegal income or the illegal income is less than 10,000 yuan, a fine of more than 30,000 yuan and less than 10,000 yuan may be imposed concurrently.

Article 37 The operator **of** critical information infrastructure violates the provisions of Article 8.7, Paragraph 1 of this law, fails to use commercial passwords as required, or fails to perform commercial password application security as required In case of sexual evaluation, the password management department shall order correction and give a warning; if it refuses to make correction or causes harm to network security, a fine of more than 10,000 yuan and less than one million yuan shall be imposed, and the directly responsible supervisor shall be imposed The employee shall be fined not less than 10,000 yuan but not more than 10,000 yuan.

Operators of critical information infrastructure who violate the provisions of Article VIII, Article 7(2) of this law and use products or services that have not been reviewed or passed the security review shall be ordered by the relevant competent authority Suspension of use, impose a fine of more than one time and less than one time of the purchase amount; impose a fine of more than 10,000 yuan and less than 10,000 yuan on the directly responsible supervisor and other directly responsible personnel.

Article 3 Violation of the provisions of **Article 2** of this law to implement import permits and export controls, and enter or exit commercial passwords shall be punished by the competent commerce department of the State Council or the customs in accordance with the law.

Article 39 In violation of the provisions of Article **9 of** this law, those who have not been identified to engage in electronic, government, and electronic authentication services shall be ordered by the password management department to correct or stop illegal actions, and give warnings. Collect illegal products and illegal income; if the illegal income is more than 30,000 yuan, a fine of one to three times the illegal income may be imposed; if there is no illegal income or the illegal income is less than 30,000 yuan, you can A fine of not less than 10,000 yuan but not more than 30,000 yuan shall also be imposed.

Article 4 Staff of the password management department and relevant departments and units abuse their powers, neglect their duties, engage in malpractices for personal gains, or disclose or provide illegal provision to others for their duties in the password operation If the business secrets and personal privacy are known to the public, they shall be punished in accordance with the law.

Article 4: Anyone who violates the provisions of this law and constitutes a crime shall be investigated for criminal responsibility according to law; if damage is caused to others, civil liability shall be borne according to law.

Chapter 5 Supplementary Provisions

Article 4 The national password management department shall formulate password management regulations in accordance with the provisions of laws and political regulations.

The fourth and third article: The measures for the management of cryptographic operations of the Chinese People's Liberation Army and the Chinese People's Armed Police Force shall be formulated by the Central Military Commission in accordance with this law.

The fourth four articles: This law will be implemented from January 1st, 2020.