Page 1

Set as homepage Add to Favorites Mobile version raditional Chinese

自立 The authoric atilbatwork communities atilities atilbatwork communities at

Network Security Review Measures

Source: Chinese Letter

April 27, 2020 12:00

(print) [Error correction]

Wechat QR code

Scan the code to enter the mobile version

No. 6

National Internet Information Office, National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Finance, Ministry of Finance, Ministry of Commerce, China People's Bank of China, National Market Supervision and Administration

The State Administration of Science and Technology, the State Administration of Radio and Television, the State Security Administration jointly formulated the "Network Security Review Measures", which are hereby promulgated.

Zhuang Rong, Director of the National Internet Information Office

The National Development and Reform Commission leads He Feng

Miao Wei, Minister of Industry and Information Technology

Minister of Public Security Zhao Kezhi

Minister of National Security Chen Qing

Minister of Finance Liu Kun

Chang Yi Gang, People's Bank of China

Minister of Commerce Zhong

Xiao Yaqing, Director of the State Administration for Market Regulation

Nie Xi, Director of the State Administration of Radio and Television

Director of the State Secrecy Bureau, Jing

Director of the National Cryptography Administration Li Zhaozong

April 2020月13日

Network Security Review Measures

Article 1 In order to ensure the security of the critical information infrastructure supply chain and maintain national security, this article is formulated in accordance with the National Security Law of the People's Republic of China and the Network Security Law of the People's Republic of China.

Method.

Article second shot of critical information infrastructure operators (hereinafter referred to as the operator) procurement of products and services Open networks, affect or may affect national security, should be in accordance with the approach into 行 Open networks security review.

Article 3 Network security review adheres to the combination of preventing network security risks and promoting the application of advanced technology, the process of fairness and transparency and the protection of intellectual property rights, the combination of pre-review and continuous supervision, The company promises to combine with social supervision to conduct reviews in terms of product and service safety and possible national security risks.

Article 4 Under the leadership of the Central Network Security and Informatization Committee, the National Internet Information Office, in conjunction with the National Development and Reform Commission of the People's Republic of China, and the People's Republic of China Industry and Information Technology

Ministry of Information and Chemistry, Ministry of Public Security of the People's Republic of China, Ministry of Security of the People's Republic of China, Ministry of Commerce of the People's Republic of China, China People's Bank of China, National Market Supervision and Administration of Public Administration of Public Administration, the State Administration have established a national network security review mechanism.

The Network Security Review Office is located in the National Internet Information Office, and is responsible for formulating related systems and regulations for network security reviews and organizing network security reviews.

Article 5 When an operator purchases network products and services, it shall predict the national security risks that may be caused by the products and services after the products and services are put into use. If it affects or may affect national security, The Office of Network Security Review has applied for a network security review.

The critical information infrastructure protection work department can formulate pre-judgment guidelines for the industry and the field.

**Article 6** For the procurement activities declared for network security review, operators shall request product and service providers to cooperate with the network security review through procurement documents, agreements, etc., including the promise of unfavorable use of the product. The convenience conditions for products and services are illegal to obtain user data, illegally control and manipulate user equipment, and do not interrupt product supply or necessary technical support services without justifiable reasons.

Article 7 When applying for a network security review, an operator shall submit the following materials:

(1) Declaration form;

(二) An analysis report that affects or may affect national security;

(3) Procurement documents, agreements, contracts to be signed, etc.;

(4) Other materials required for network security review.

Article 1 The Network Security Review Office shall, upon receipt of the review application materials, determine whether review is necessary and notify the operator in writing within 10 working days.

Article 9 The network security review focuses on assessing the national security risks that may be brought about by the procurement of network products and services, mainly considering the following factors:

(1) The risks of critical information infrastructure being illegally controlled, being disturbed or destroyed, and important data being stolen, leaked, or destroyed after the use of products and services;

(二) The damage to the business continuity of critical information infrastructure caused by the interruption of product and service supply;

(3) The safety, openness, transparency, diversity of sources of products and services, the reliability of supply channels, and the risk of supply interruption due to political, diplomatic, trade and other factors;

(4) Product and service providers' compliance with Chinese laws, political regulations, and departmental rules;

(5) Other factors that may endanger the security of critical information infrastructure and national security.

Article 10 If the Network Security Review Office considers that it is necessary to conduct a network security review, it shall complete the preliminary review within 30 days from the date of issuing a written notice to the operator, including the conclusion of the review.

Discuss the recommendations and send the review conclusions and recommendations to the member units of the network security review work mechanism and relevant key information infrastructure protection work departments for comments; if the situation is complicated, 15 work can be extended.

Article 10 The member units of the network security review work mechanism and the relevant critical information infrastructure protection work departments shall respond to their opinions in 15 working days from the date of receipt of the review conclusions and recommendations.

If the member units of the network security review work mechanism and relevant critical information infrastructure protection work departments agree, the network security review office will notify the operator of the review conclusion in written form;

If the opinions are inconsistent, it shall be handled in accordance with the special review procedure and the operator shall be notified.

Article 2 In case of processing in accordance with special review procedures, the Cyber Security Review Office shall listen to the opinions of relevant departments and units, conduct in-depth analysis and evaluation, and form review conclusions and recommendations again, and solicit

Opinions of member units of the network security review mechanism and related critical information infrastructure protection work departments shall be submitted to the Central Network Security and Informatization Committee for approval in accordance with the procedures, and the review conclusions shall be formed and documented Notify the operator.

Article 3 The special review procedure should generally be completed within 45 working days, and can be extended appropriately if the situation is complicated.

Article 4 If the Network Security Review Office requires supplementary materials, operators, product and service providers shall cooperate. The time for submitting supplementary materials does not count towards the review time.

Article 5 The network security review work mechanism member units believe that the network products and services that affect or may affect national security shall be reported to the central network security and information by the network security review office in accordance with procedures.

After approval by the Information and Chemical Committee, the review shall be conducted in accordance with the provisions of these Measures.

Article 6: Relevant institutions and personnel participating in network security reviews shall strictly protect the business secrets and intellectual property rights of enterprises, and review the undisclosed materials submitted by operators, product and service providers, and review.

Other undisclosed information learned in the investigation shall be kept confidential; without the consent of the information provided, it shall not be disclosed to unrelated parties or used for purposes other than review.

Article VII: Operators or network product and service providers who believe that the reviewers are not objective and fair, or fail to undertake the confidentiality obligation for the information learned during the review, may apply for a network security review Report from the office or related departments.

Article 10 Operators shall supervise and urge product and service providers to fulfill the commitments made in the network security review.

The Cyber Security Review Office strengthened the supervision before and after the incident by accepting reports and other forms.

Article 9: If an operator violates the provisions of these Measures, it shall be dealt with in accordance with Article 6.5 of the "Network Security Law of the People's Republic of China".

Article 2 The key information infrastructure operator in these Measures refers to the operator recognized by the key information infrastructure protection department.

The network products and services mentioned in these Measures mainly refer to nuclear network equipment, high-performance computers and servers, large-capacity storage equipment, large-scale databases and application software, network security equipment, and cloud computing Services, and other network products and services that have an important impact on the security of critical information infrastructure.

Article 2 involving state secret information shall be implemented in accordance with the relevant state confidentiality regulations.

Article 2 This method will be implemented from June 1st, 2020, and the "Measures for the Security Review of Network Products and Services (Trial)" will be repealed at the same time.