Translation

The following regulation, issued by the Cyberspace Administration of China (CAC) in 2020, affects PRC companies that run China's "critical information infrastructure." The regulation requires operators of key PRC network platforms to undergo a CAC cybersecurity review before launching products or services that may impact Chinese national security.

Title
Measures for Cybersecurity Reviews
网络安全审查办法

Signatories
Zhuang Rongwen (庄荣文), director of the Cyberspace Administration of China (CAC; 国家互联网信息办公室; 网信办); He Lifeng (何立峰), director of the National Development and Reform Commission (NDRC; 国家发展和改革委员会; 发改委); Minister of Industry and Information Security (MIIT; 工业和信息化部; 工信部) Miao Wei (苗圩); Minister of Public Security (公安部部长) Zhao Kezhi (赵克志); Minister of State Security (MSS; 国家安全部部长) Chen Wenqing (陈文清); Minister of Finance (财政部部长) Liu Kun (刘昆); Minister of Commerce (商务部部长) Zhong Shan (钟山); Yi Gang (易纲), governor of the People's Bank of China (PBOC; 中国人民银行); Xiao Yaqing (肖亚庆), director of the State Administration for Market Regulation (国家市场监督管理总局); Nie Chenxi (聂辰席), director of the National Radio and Television Administration (NRTA; 国家广播电视总局); Tian Jing (田静), director of the National Administration of State Secrets Protection (国家保密局); and Li Zhaozong (李兆宗), director of the State Cryptography Administration (国家密码管理局).

Source
China Cybersecurity Review Technology and Certification Center (中国网络安全审查技术与认证中心) website. The *Measures* are dated April 13, 2020 and were uploaded to the website on May 11, 2020.

The Chinese source text is available online at:
https://isccc.gov.cn/images/zxyw/cprz/wlaqsc/zcwj/2020/05/11/0F1F6BDCA010C8C7D0138724EFDF442B.pdf
An archived version of the Chinese source text is available online at: https://perma.cc/S6A3-257H

Translation Date	**Translator**	**Editor**
January 25, 2021	Etcetera Language Group, Inc.	Ben Murphy, CSET Translation Lead

Order of the Cyberspace Administration of China (CAC), the National Development and Reform Commission (NDRC), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security, the Ministry of State Security (MSS), the Ministry of Finance, the Ministry of Commerce, the People's Bank of China (PBOC), the State Administration for Market Regulation, the National Radio and Television Administration (NRTA), the National Administration of State Secrets Protection, and the State Cryptography Administration

No. 6

CAC, NDRC, MIIT, the Ministry of Public Security, MSS, the Ministry of Finance, the

Ministry of Commerce, PBOC, the State Administration for Market Regulation, NRTA, the National Administration of State Secrets Protection, and the State Cryptography Administration have jointly formulated and hereby promulgate the *Measures for Cybersecurity Reviews*.

CAC Director	Zhuang Rongwen
NDRC Director	He Lifeng
Minister of Industry and Information Technology	Miao Wei
Minister of Public Security	Zhao Kezhi
Minister of State Security	Chen Wenqing
Minister of Finance	Liu Kun
Minister of Commerce	Zhong Shan
PBOC Governor	Yi Gang
Director of the State Administration for Market Regulation	Xiao Yaqing
NRTA Director	Nie Chenxi
Director of the National Administration of State Secrets Protection	Tian Jing
Director of the State Cryptography Administration	Li Zhaozong

April 13, 2020

Measures for Cybersecurity Reviews

Article 1 In order to ensure the security of critical information infrastructure supply chains and to maintain national security, these measures have been formulated in accordance with the *National Security Law of the People's Republic of China* and the *Cybersecurity Law of the People's Republic of China*.

Article 2 Critical information infrastructure operators (hereinafter "operators") that procure network products and services that impact or can impact national security shall conduct cybersecurity reviews in accordance with these Measures.

Article 3 Cybersecurity reviews shall persist in combining defense against cybersecurity risks with promotion of advanced technology applications, combining fair and transparent processes with the protection of intellectual property (IP), combining ex-ante review with ongoing monitoring, and combining promises by enterprises with monitoring by society in conducting security reviews on all products and services that may bring about national security risks.

Article 4 Under the leadership of the Central Cyberspace Affairs Commission, CAC will work with NDRC, MIIT, the Ministry of Public Security, MSS, the Ministry of Finance, the Ministry of Commerce, PBOC, the State Administration of Market Regulation, NRTA, the National Administration of State Secrets Protection, and the State Cryptography Administration to establish mechanisms for national cybersecurity review work.

The Cybersecurity Review Office (网络安全审查办公室) is established under CAC and is responsible for formulating relevant regulations for cybersecurity reviews and organizing cybersecurity reviews.

Article 5 When operators procure network products and services, they shall forecast the potential national security risks that may arise from the use of the products and services. When products and services impact or may impact national security, operators shall apply to the Cybersecurity Review Office for cybersecurity review.

Critical information infrastructure protection work departments can formulate forecasting guidelines for their industries and fields.

Article 6 For procurement activities that have applied for cybersecurity review, operators shall require the product and service providers to cooperate with the cybersecurity review by providing procurement documents, agreements, and other such contracts. This shall include commitments not to use the expedient of providing products and services to illegally obtain user data, illegally control or manipulate user equipment, or interrupt product supply or necessary technical support services without justifiable reasons.

Article 7 When reporting for cybersecurity review, operators shall submit the following materials:

(1) Application form;

(2) Analysis report on the impact or potential impact on national security;

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

(4) Other materials required for the cybersecurity review work.

Article 8 The Cybersecurity Review Office shall determine whether or not a review is required and issue a written notice to the operator within 10 business days from the receipt of the review report materials.

Article 9 The cybersecurity review focuses on assessing the potential national security risks posed by the network products and services to be procured, primarily considering the following factors:

(1) The risks of illegal control, interference, or destruction of critical information infrastructure and the theft, disclosure, or destruction of important data caused by the use of the products and services;

(2) The danger that disruption to the supply of the products and services pose to the operational continuity of critical information infrastructure;

(3) Product and service security, openness, transparency, diversity of sources, supply chain reliability, and risk of supply disruption due to political, diplomatic, trade, and other such factors;

(4) The compliance of product and service providers with Chinese laws, administrative regulations, and departmental rules.

(5) Other factors that may threaten the security of critical information infrastructure or national security.

Article 10 When the Cybersecurity Review Office recognizes that a cybersecurity review must be conducted, it shall complete the preliminary review within 30 business days of issuing the written notice to the operator. This includes the formation of review conclusions and recommendations and sending the review conclusions and recommendations to the member units of the cybersecurity review work mechanism and relevant critical information infrastructure

protection work departments for comments. In complex cases, this period can be extended by 15 business days.

Article 11 Member units of the cybersecurity review work mechanism and relevant critical information infrastructure protection work departments shall reply with comments in writing within 15 business days of the receipt of the review conclusions and recommendations.

When the comments of member units of the cybersecurity review work mechanism and relevant critical information infrastructure protection work departments are in agreement, the Cybersecurity Review Office shall notify the operator of the review conclusion in writing. If the comments show disagreement, the matter shall be handled according to a special review procedure and the operator shall be notified.

Article 12 For cases handled according to special review procedures, the Cybersecurity Review Office shall listen to the comments of relevant departments and units, carry out in-depth analysis and assessment, and reformulate its review conclusions and recommendations. It shall then solicit comments from member units of the cybersecurity review work mechanism and relevant critical information infrastructure protection work departments. After reporting to the Central Cyberspace Affairs Commission for approval in accordance with the procedures, it shall form a review conclusion and notify the operator in writing.

Article 13 Generally, the special review procedure shall be completed within 45 business days. This period may be extended for complex cases.

Article 14 When the Cybersecurity Review Office requires the provision of additional information, the relevant operators and product and service providers shall cooperate. The time for the submission of additional materials is not included in the review time.

Article 15 When member units of the cybersecurity review work mechanism believe that network products and services impact or can impact national security, the Cybersecurity Review Office shall report the matter to the Central Cyberspace Affairs Commission for approval in accordance with procedures. Then, a review shall be conducted in accordance with the provisions of these Measures.

Article 16 Relevant institutions and personnel that participate in cybersecurity reviews shall strictly protect the trade secrets and IP of enterprises and shall bear secrecy protection obligations as to the not-yet publicly disclosed materials submitted by operators and product and service providers and other not-yet publicly disclosed information they have access to in their review work. Without the consent of the information provider, they shall not disclose such information to an unrelated party or use it for any purpose other than the review.

Article 17 When an operator or network product and service provider believes that a reviewer is not objective or fair or cannot honor secrecy protection obligations as to the information accessible during the review, the operator or provider can report the issue to the Cybersecurity Review Office or relevant department.

Article 18 Operators shall supervise and urge product and service providers to fulfill their commitments made during the cybersecurity review.

The Cybersecurity Review Office shall strengthen supervision before, during, and after relevant activities by accepting reports [on problems] and through other formats.

Article 19 Operators that violate the provisions of these Measures shall be dealt with in

accordance with Article 65 of the *Cybersecurity Law of the People's Republic of China*.

Article 20 In these Measures, "critical information infrastructure operators" refers to the operators so designated by critical information infrastructure protection work departments.

For the purpose of these Measures, "network products and services" primarily refers to core network equipment, high-performance computers and servers, high-capacity storage equipment, large databases and application software, cybersecurity equipment, cloud computing services, and other network products and services that have an important impact on the security of critical information infrastructure.

Article 21 Matters involving state secrets shall be carried out in accordance with the relevant state secrecy protection regulations.

Article 22 These Measures shall be implemented from June 1, 2020, simultaneously repealing the *Measures for Security Review of Network Products and Services (for Trial Implementation)*.