# Measures on Cybersecurity Review

Dan Young Business Consultancy — www.danyoungcpa.com

Unofficial English translation prepared for reference only. The official Chinese text prevails.

## Measures on Cybersecurity Review

### Article 1

These Measures are formulated in accordance with the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Law of the People's Republic of China on the Protection of Critical Information Infrastructure, and other applicable laws and regulations, for the purpose of ensuring cybersecurity and data security, safeguarding national security, protecting the lawful rights and interests of the people, and promoting the lawful, orderly, and free flow of data.

### Article 2

These Measures apply to the cybersecurity review conducted by the Cybersecurity Review Office in accordance with the law, where a critical information infrastructure operator procures network products and services, or a network platform operator conducts data processing activities that affect or may affect national security. For the purposes of the preceding paragraph, a "network platform operator" means any operator providing online information services that possess the personal information of more than one million users.

### Article 3

Under the leadership of the Central Cybersecurity and Informatization Commission, the national cybersecurity review working mechanism shall be responsible for formulating cybersecurity review policies, organizing cybersecurity reviews, and supervising the implementation of these Measures. The Cybersecurity Review Office established within the Cyberspace Administration of China (CAC) shall be responsible for the day-to-day work of cybersecurity review.

### Article 4

When procuring network products and services, critical information infrastructure operators shall anticipate the potential national security risks that the products and services may pose after being put into use. Where the procurement affects or may affect national security, a cybersecurity review shall be applied for from the Cybersecurity Review Office. Where a cybersecurity review is required, the operator shall apply for the review before entering into a procurement contract with the product or service provider.

### Article 5

Where a critical information infrastructure operator procures network products and services that affect or may affect national security, the operator shall consider the following factors when assessing national security risks:

(1) the risks of the products and services being used to illegally control, interfere with, or disrupt critical information infrastructure, or illegally obtain, exploit, disclose, or destroy relevant data;

(2) the possibility that the supply of products and services may be interrupted, affecting the continuous, safe, and stable operation of critical information infrastructure;

(3) the security, openness, transparency, and diversity of the sources of products and services, and the reliability of the supply channels;

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



Source: https://www.danyoungcpa.com/cybersecurity-review-measures-english-translation/

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

### Article 6

Where a network platform operator possesses the personal information of more than one million users and plans to list abroad, it shall apply for a cybersecurity review from the Cybersecurity Review Office. The operator shall apply for cybersecurity review before submitting an application for listing abroad to the relevant overseas securities regulatory authorities.

### Article 7

Where a network platform operator possesses the personal information of more than one million users, or where a network platform operator that has listed abroad or plans to list abroad undertakes any of the following activities that affect or may affect national security, the Cybersecurity Review Office may initiate a cybersecurity review ex officio:

(1) engaging in data processing activities that affect or may affect national security, including the collection, storage, use, processing, transmission, provision, or disclosure of data;

(2) cross-border transfer of data that affects or may affect national security; or

(3) other activities that affect or may affect national security as determined by the Cybersecurity Review Office.

### Article 8

Where it is necessary to conduct a cybersecurity review of a network platform operator that possesses the personal information of more than one million users on account of its data processing activities affecting or may affect national security, the Cybersecurity Review Office shall report the matter to the Central Cybersecurity and Informatization Commission for approval before initiating the review.

### Article 9

To apply for a cybersecurity review, the operator shall submit the following materials:

(1) a cybersecurity review application form;

(2) an analysis report on the national security risks that the network products and services to be procured, or the data processing activities, or the overseas listing, may pose;

(3) a risk mitigation plan or measures to be taken;

(4) other materials required for the cybersecurity review.

### Article 10

The Cybersecurity Review Office shall, within 10 working days of receiving the application materials, preliminarily determine whether the materials meet the review requirements and notify the operator in writing. If the requirements are met, the Cybersecurity Review Office shall accept the application and initiate the review. If the application materials are incomplete, the Cybersecurity Review Office shall notify the operator to supplement them. The operator shall complete the supplementation within 10 working days.

### Article 11

Where the Cybersecurity Review Office considers that the reported matter involves national security risks, it shall, within 30 working days of accepting the application for review, complete the preliminary review. The period for submitting supplementary materials by the operator shall not be included in the review period.

### Article 12

After completing the preliminary review, the Cybersecurity Review Office shall forward the review opinions and the operator's application materials to the members of the cybersecurity review working mechanism and the relevant departments of the State Council for comments. The members of the cybersecurity review working mechanism and the relevant departments shall provide written comments to the Cybersecurity Review Office within 15 working days. Where the opinions of the members of the cybersecurity review working mechanism and the relevant departments are inconsistent, the Cybersecurity Review Office shall report the matter to the Central Cybersecurity and Informatization Commission for a decision in accordance with the prescribed procedures.

### Article 13

Under special circumstances, the time limit for the cybersecurity review may be extended by 15 working days. Under particularly complex circumstances, the time limit may be further extended upon approval.

### Article 14

The cybersecurity review shall focus on assessing the following national security risk factors concerned with the operator's procurement of network products and services, data processing activities, or overseas listing:

(1) the risks of core data, important data, or large amounts of personal information being stolen, leaked, destroyed, illegally used, or transferred abroad;

(2) the risks that the operator's procurement of network products and services, data processing activities, or overseas listing may pose to critical information infrastructure, core data, or important data security;

(3) the risks that the operator's procurement of network products and services, data processing activities, or overseas listing may pose to national security in key information infrastructure sectors, including but not limited to national defense, military industry, or critical strategic sectors;

(4) the risks that the products and services provided by the operator after overseas listing may be used by foreign governments to maliciously influence, control, or interfere with China's cyberspace operations; and

(5) other factors that may endanger cybersecurity or national security as determined by the relevant state authorities.

### Article 15

Upon completion of the cybersecurity review, the Cybersecurity Review Office shall notify the operator of the review decision in writing. The review decision shall be one of the following:

(1) approval, meaning no material national security risks are found;

(2) conditional approval, meaning the operator is required to take corrective measures to effectively mitigate the identified risks; or

(3) disapproval, meaning material national security risks are found.

### Article 16

Where the cybersecurity review reaches a conclusion of conditional approval, the operator shall, within the time limit specified by the Cybersecurity Review Office, implement the required corrective measures and report the implementation results in writing. The Cybersecurity Review Office shall verify the effectiveness of the corrective measures taken by the operator.

### Article 17

Where an operator applying for cybersecurity review or the relevant product or service provider disagrees with the review decision, the Cybersecurity Review Office shall, upon request, provide an explanation. Where the operator still disagrees, it may submit a complaint to the Central Cybersecurity and Informatization Commission in accordance with the prescribed procedures.



Source: https://www.danyoungcpa.com/cybersecurity-review-measures-english-translation/

### Article 18

Operators shall cooperate with the cybersecurity review and provide truthful materials. Where an operator refuses to cooperate, provides false materials, or otherwise obstructs the cybersecurity review, the Cybersecurity Review Office shall report to the relevant authorities for handling in accordance with the law.

### Article 19

Participants in the cybersecurity review, including staff members of the Cybersecurity Review Office, members of the working mechanism, experts, and other relevant personnel, shall keep confidential the trade secrets, personal privacy, and other information of the operator that they become aware of in the course of performing their duties. They shall not disclose, illegally provide, or use such information.

### Article 20

Where a critical information infrastructure operator or a network platform operator violates the provisions of these Measures by failing to apply for a cybersecurity review as required, or by using the relevant network products and services before the cybersecurity review is completed, the relevant competent authorities shall impose penalties in accordance with the Cybersecurity Law, the Data Security Law, and other applicable laws and administrative regulations.

### Article 21

For the purposes of these Measures:

(1) “Critical information infrastructure” means critical information infrastructure as defined in the Regulations on the Security Protection of Critical Information Infrastructure.

(2) “Network products and services” includes core network equipment, high-performance computers and servers, large-capacity storage equipment, large databases and application software, cybersecurity equipment, cloud computing services, and other network products and services that have a material impact on the security of critical information infrastructure.

### Article 22

Where, before the implementation of these Measures, a network platform operator has already submitted an application for listing abroad, it shall, in accordance with the requirements of the national cyberspace administration authority, make the appropriate supplemental application for cybersecurity review.

### Article 23

These Measures shall come into force on February 15, 2022. The Measures on Cybersecurity Review issued on April 13, 2020 shall be repealed simultaneously.

Disclaimer: This is an unofficial English translation provided for reference and informational purposes only. While every effort has been made to ensure accuracy, only the official Chinese version published by the National People’s Congress (NPC) or the State Council of the People’s Republic of China carries legal force. For legal matters, please consult a qualified professional. For official legal advice specific to your situation, contact Dan Young Business Consultancy.