NEWSLETTER
LIFANG & PARTNERS 立方观评
关注更多精彩内容
No.138
2020.04
SPECIAL ISSUE

China to Tighten its Teeth on Cybersecurity Regulation

New Rule for Critical Information Infrastructure Operators

On April 27, 2020, 12 departments in China, including the Cyberspace Administration of China ("**CAC**"), the National Development and Reform Commission, the Ministry of Public Security, jointly released the *Cybersecurity Review Measures* ("***Measures***"), which will come into force on 1 June 2020 and will replace the *Measures on Security Examination for Online Products and Services (Trial Implementation)* ("***Trial Implementation***") simultaneously. Comparing to the 2017 *Trial Implementation* and the *Exposure Draft* of *Cybersecurity Review Measures* released in 2019, this newly released version is revised from many perspectives.

Based on the *State Security Law* and the *Cybersecurity Law*, the new *Measures* stipulates the cybersecurity review mechanism for a critical information infrastructure operator ("**CIIO**") to purchase network products and services. Before purchasing, the CIIO shall assess the possible risks to national security after such product and service are put into use. If they affect or are likely to affect national security, the CIIO shall apply for the cybersecurity review in advance. In combination with the statements of CAC's officials on relevant issues during a press conference ("**CAC Official's Statement**") on April 27, the *Measures* specified the following eight issues in connection with the security review:

Issue 1: Who need to apply for the security review?

The CIIO, as a purchaser of network products and services, is the notifying party and liability entity. Comparing to the 2017 Trial Implementation, the Measures is more concerned with the supply-chain security of a CIIO. CAC Official's Statement identified some critical industries, including telecommunications, radio & TV, energy, finance, transportation of highway, waterway and railway, civil aviation, postal service, water projects, emergency management, healthcare, social security, defense science and technology, etc., in which the CIIO shall consider applying for cybersecurity review pursuant to the Measures when purchasing network products and services.

Issue 2: What kinds of products will be subject to the security review?

The CIIO shall apply for the cybersecurity review when purchasing core network equipment, high-performance computers and servers, large-capacity storage equipment, large databases and application software, network security equipment, cloud computing services, and other network product or service that have a significant impact on the security of critical information infrastructure.

Issue 3: Who is responsible for the security review?

The Measures stipulates that the Cybersecurity Review Office, a subdivision of the CAC, will be responsible for the acceptance and preliminary review of the cybersecurity review applications. Members of the cybersecurity review working mechanism and relevant departments for protection of critical information infrastructure will assist in the review. In the special review process, a suggested finding shall also be reported to the Central Cyberspace Affairs Commission for approval. According to CAC Official's Statement, the China Cybersecurity Review Technology and Certification Center will be responsible for specific work, including the reception of notification materials, formal review of the notification materials and the organization of review, etc.

Issue 4: When to apply for the security review?

The Measures stipulates the notification mechanism of the cybersecurity review that the CIIO shall apply for the cybersecurity review actively in advance if prejudging that uses of purchasing products and services have potential risks to national security. CAC Official's Statement indicated that, in general, the cybersecurity review is required before a CIIO signing the purchase contract with the supplier of relevant product and service. If the review applied after the signing of the contract, it is suggested to indicate in the contract that the contract shall not take effect until the purchase of products and services has passed the cybersecurity review.

Issue 5: What notification materials need to be prepared?

In accordance with the Measures, the CIIO shall submit the following materials to apply for the security review:

a notification statement;

an analysis report concerning the impact or possible impact on national security;

the procurement document, agreement, contract to be concluded, etc.; and;

other materials required for the cybersecurity review.

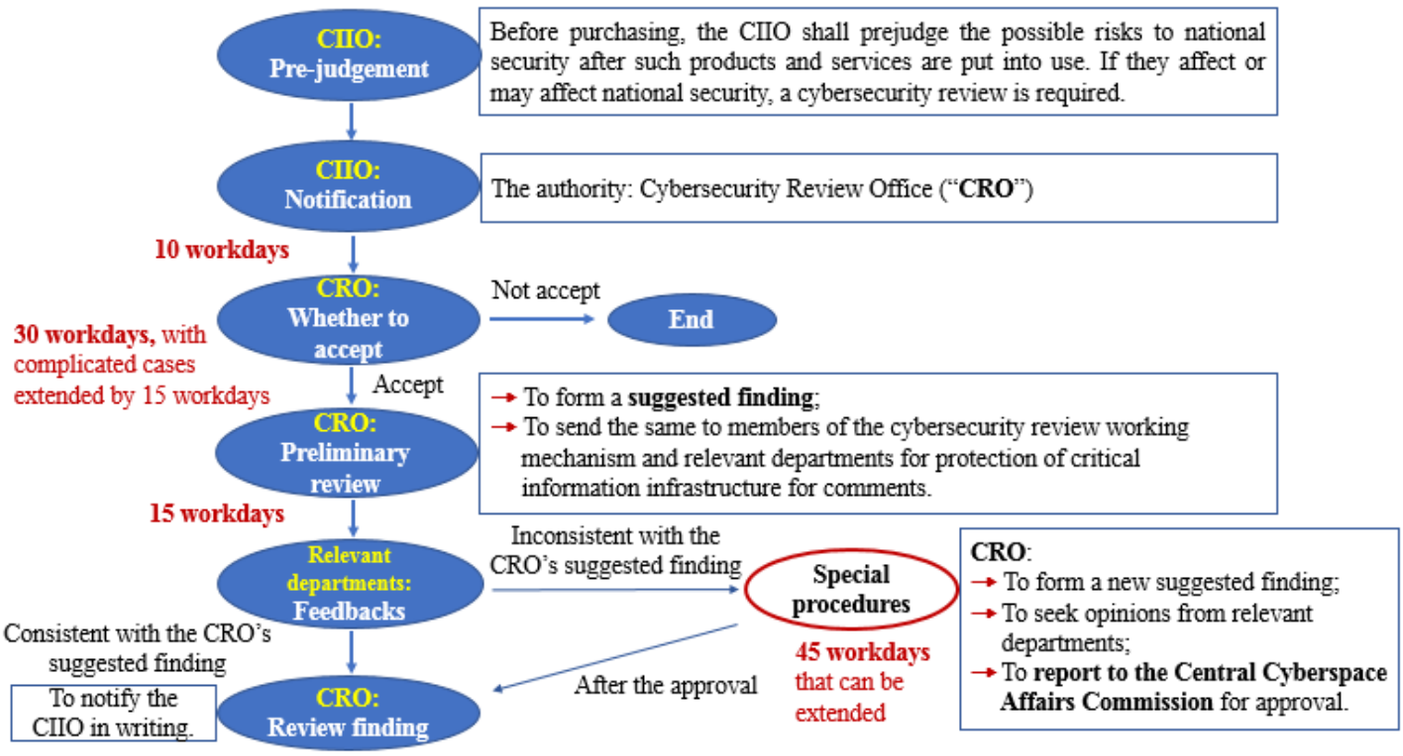
Currently, there is no template of such files has been released.

Issue 6: What are the factors to be assessed during the security review?

Based on the evaluation of possible risks to national security caused by the purchase of the network products and services, the cybersecurity review shall assess the following five factors: (i) the risks to be caused by the use of product and services that the critical information infrastructure to be illegally controlled, interfered with or destroyed, or that important data are stolen, leaked or destroyed; (ii) damages to the continuity of critical information infrastructure business caused by supply interruption of the product and service; (iii) safety, openness, transparency, and diversity of sources of the product and service, reliability of supply channels, and risks of supply interruption as a result of political, diplomatic, trade or any other factors; (iv) compliance with Chinese laws, administrative regulations and departmental rules by the product and service provider, which highlights the importance of compliance operation in China, and; (v) other factors that may endanger the security of the critical information infrastructure or the national security. The Measures sets "other factors" as the bottom line, giving the competent authorities broad discretion.

Issue 7: What is the process and timeframe of security review?

The Measures clarifies the process of cybersecurity review to include four stages: the acceptance, the preliminary review, feedbacks, the special review process (not necessary). The normal process will take 45 workdays, with complicated cases extended by 15 workdays. If entering the special review process, it may take another 45 workdays or more. It is worthy of noting that the time for providing supplementary materials will not be counted.



Issue 8: What are the consequences and responsibilities of violations?

The Measures clarifies the consequences and responsibilities of violations. The CIIO who violates the Measures shall be dealt with pursuant to the Article 65 of the Cybersecurity Law. The CIIO, who shall apply for the cybersecurity review but fail to do so, or using products and/or services which have not undergo or have failed in the cybersecurity review, shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than 1 but less than 10 times the purchase price, and the supervisor directly in charge and other directly liable persons shall be subject to a fine of ranging from RMB 10,000 yuan to 100,000 yuan.

Subscribe to our WeChat community

Beijing | Shanghai | Wuhan | Guangzhou | Shenzhen | Korea

www.lifanglaw.com
Email：info@lifanglaw.com
Tel：+8610 64096099
Fax：+8610 64096260/64096261