China Issued the Measures for Cybersecurity Review

Wednesday, April 29, 2020

The Cyberspace Administration of China ("CAC"), together with 11 other authorities, has jointly issued the Measures for Cybersecurity Review (the "Measures"), which will take effect on June 1, 2020, and the currently-effective Measures for Examining the Security of Network Products and Services will be repealed simultaneously.

The Measures, developed on the basis of State Security Law and Cybersecurity Law, aim to ensure the safety of the supply chain of critical information infrastructure and guarantee national security. Where the purchase of network products and services by an operator of critical information infrastructure (the "Operator") influences or may influence state security, the Operator shall notify the Cybersecurity Review Office, which is under the CAC, and a cybersecurity review shall be conducted pursuant to the Measures. Based on the Measures, an Operator shall be recognized by the relevant department as protecting critical information infrastructure.

During a cybersecurity review, the state security risk, which may be generated by the purchase of network products and services, will be evaluated and the following factors taken into consideration (among others):

- the risk of illegal control over, disturbance or destruction of critical information infrastructure and the risk of critical data being stolen, divulged or damaged after the use of products and services;
- damage to the continuity of critical information infrastructure business, due to
interruption of supply for the products or services;

- the security, openness, transparency and the diversity of sources of products or services, the dependability of the supply chain, and the risk of supply interruption due to factors such as politics, diplomacy or trade;

- conditions of compliance with state laws, administrative regulations and department rules by the provider of products or services; and

- other factors which may endanger the safety of critical information infrastructure and state security.

In declaring a purchase for a cybersecurity review, the Operator shall submit the following materials: (1) a declaration statement; (2) the analysis report of the effect or possible effect on state security; (3) a purchase document, agreement or contract intended to be signed, etc.; and (4) other materials required by a cybersecurity review.

According to the Measures, during purchase activity with a cybersecurity review having been declared, the Operator shall require the provider of products or services, via a purchase document or agreement, to coordinate the cybersecurity review. This includes not illegally acquiring user data, or illegally controlling or manipulating user facilities using advantageous position of providing products and services, and not interrupting the supply of products or necessary technical support services without justification.

The Cybersecurity Review Office shall provide written notification to the relevant Operator if it thinks a cybersecurity review is required and shall complete the preliminary review within 30 working days of such written notification. The time limit may be extended by 15 working days if the case is complicated. As for special review, it shall be completed within 45 working days normally, but the time limit may be extended if the case is complicated. The time for supplemental document submission is not included in these time limits.

According to the Measures, the relevant organizations and personnel involved in the cybersecurity review shall maintain strict confidentiality with regard to the commercial secrets and intellectual property rights of the enterprises. They shall also bear responsibility for the confidentiality of nonpublic materials submitted by operators and other nonpublic information acknowledged during the review, and must not disclose to any irrelevant party, nor for purposes other than the review.

Under Article 65 of the Cybersecurity Law, where operators of critical information infrastructure use network products or services that have neither been reviewed for security, nor passed the cybersecurity review, they shall be ordered by the relevant competent departments to stop using such products or services, and a fine of no less than one, but no more than ten times the purchase amount shall be imposed. As for the persons directly in charge or otherwise directly responsible, a fine of no less than RMB 10,000 but no more than RMB 100,000 shall be imposed.

Copyright © 2020, Hunton Andrews Kurth LLP. All Rights Reserved.