Akin®

China Issues New Cybersecurity Review Measures

Jun 4, 2020

Reading Time : **3 min**

By: Jingli Jiang

Subjects and Applicants of the Cybersecurity Review:

Where the purchase of network products and services by an operator of critical information infrastructures (the "CII operator") influences or may influence state security, a cybersecurity review shall be conducted pursuant to Article 2 of the Review Measures. According to the FAQ of the Review Measures (find the FAQ here in Chinese), the CII operator includes the operators of important networks and information systems in the fields of telecommunications, radio and television, energy, finance, road and water transportation, railways, civil aviation, postal services, water conservancy, emergency management, health and wellness, social security, defense technology industry, etc. According to Article 20 of the Review Measures, the governmental department for the protection of critical information infrastructures will finally identify the CII operator.

When purchasing network products or services, the CII operator shall consider whether potential state security risks may arise after the use of such products or services. If the state security can be affected or may be affected, the CII operator shall declare the procurement to the cybersecurity review office to conduct a cybersecurity review. The pre-judgment guideline for the CII operators may be formulated by the department for the protection of critical information infrastructures, and before the issuance of the pre-judgment guideline, the CII operator may at least consider the primary elements listed in Article 9 of the Review Measures for the cybersecurity review (details as provided below).

Additionally, the cybersecurity review office can conduct a review on the network products or services if the review office is concerned that they can influence or may influence state

security, after getting the approval of the Central Cyberspace Affairs Commission.

The Scope of the Cybersecurity Review:

According to Article 20 of the Review Measures, the "network products and services" mainly refer to core network equipment, high-performance computers and servers, mass storage equipment, large databases and applications, network security equipment, cloud computing services and other network products and services that have an important impact on the security of critical information infrastructures.

Main Factors of the Cybersecurity Review:

According to Article 9 of the Review Measures, the state security risk will be the primary focus during a cybersecurity review, and the following factors are taken into consideration during the review:

(1) The risk of illegal control, interference or destruction of critical information infrastructures and the theft, leakage or destruction of important data that arises due to the use of the products or services.

(2) The harm caused by the disruption of the supply of products or services to the operation continuity of critical information infrastructures.

(3) The risk of the security, openness, transparency and diversity of sources of the products or services, the risk of the reliability of supply channels, as well as the risk of supply interruption due to politics, diplomacy, trade, etc.

(4) The compliance situations of the provider of products or services with Chinese laws, administrative regulations and departmental rules.

(5) Other factors which may endanger the safety of critical information infrastructures and state security.

Requirements on Relevant Contract Clauses:

According to Article 6 of the Review Measures, for procurement activities that are filed for the cybersecurity review, the relevant CII operator shall request the product and/or service providers to cooperate with the cybersecurity review, for example, committing to not illegally

obtain user data and control or illegally operate user's equipment, and to not interrupt supply or technical support service without justified reasons.

Timeline of the Cybersecurity Review:

The cybersecurity review office shall complete the preliminary review and send review conclusions and suggestions to the member authorities of the cybersecurity review mechanism and the relevant key information infrastructure protection government agencies (the "other related authorities") within 30 working days from the date of issuing the written notice to the CII operator, and the review time may be extended by 15 working days if the situation is complicated.

The other related authorities shall provide their opinions in writing within 15 working days after they receive the review conclusions and suggestions from the cybersecurity review office. If the other related authorities reach a consensus, the cybersecurity review office will send the review conclusions to the CII operator in writing; if no consensus is reached, the office will notify the CII operator and review the case under a special review procedure. This special review procedure has not been issued with the Review Measures, which may be issued by the related governmental authority later or only established as an internal undisclosed review procedure of the review office.

Categories

Cybersecurity & Information Security

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.