WINSTON & STRAWN LLP

BLOG

China Issues Draft Measures That Affect the IPOs of Chinese Companies

JULY 30, 2021

Those who follow legal trends in the People's Republic of China ("**China**" or the "**PRC**") have become accustomed to government agencies taking actions in specific industries or related to particular business activities in the period around major meetings or events. The centennial anniversary of the Chinese Communist Party was no different. The Chinese government made clear in the days following the centennial celebration its continued emphasis on protecting data within its borders.

In the last few months, several prominent Chinese companies with significant data stockpiles in China have attempted to complete or have completed their IPOs in the US only to come under the scrutiny of a data security review and investigation by the Cyberspace Administration of China. These companies and their IPOs were significantly impacted by these developments and face the difficult task of navigating the balance of disclosure requirements and compliance with Chinese regulators.

On Saturday, July 10, 2021, the PRC National Internet Information Office ("**NIIO**") issued draft Cybersecurity Review Measures (the "**Draft Measures**") for public comment. The Draft Measures are intended to protect data and national security by making mandatory cybersecurity reviews for certain companies in particular circumstances. The NIIO is accepting public comment on the Draft Measures until July 25, 2021.

The Draft Measures apply to critical information infrastructure operators[1] ("**CIIOs**") purchasing network products and services that affect or may affect national security and data processors[2] carrying out data-processing activities that affect or may affect national security. The Draft Measures refer to both CIIOs and data processors as "Operators." Many companies with significant operations in China could be considered data processors.

Under the Draft Measures, there are two types of conduct that give rise to a mandatory cybersecurity review: (1) the procurement by a CIIO of certain types of network products and services that affect or may affect national security and (2) an oversees IPO by an operator that is in possession of the personal information[3] of more than 1 million users.

Article 10 of the Draft Measures describes the main factors that the cybersecurity review will consider related to potential national-security risks. The overall concern is that China-based data and personal information could be leaked from equipment or disclosed to foreign governments during an IPO.

The timing for the release of the Draft Measures notifies Chinese companies considering or in the process of an overseas IPO (particularly those utilizing a VIE structure) that significant data protection measures and government oversight will be required. While the intent of the Draft Measures may be the data protection practices of Chinese companies, the language of the Draft Measures, with cross-referenced definitions in other PRC laws, is broad and could include foreign companies that meet the definition of operators.

Foreign companies doing business in China should know whether they are CIIOs or data processors and should periodically review compliance with the web of PRC laws governing data.

Chinese companies with significant amounts of personal information planning to go through an IPO on an overseas exchange will face new challenges to that process. Those companies should understand the types of data that will be required in the relevant locations and should balance the legal requirements for disclosure with PRC laws protecting data.

Other participants in the IPO process should utilize independent counsel to understand issues like the cybersecurity review process, the compliance of companies with PRC data laws, and the potential issues of any investigations.

[1] "Critical Information Infrastructure Operator" is defined in the PRC Cybersecurity Law as the identified operator of the division charged with the protection of critical-information infrastructure.

[2] "Data Processors" are defined as those engaged in "Data Processing" activities as defined under the PRC Data Security Law, Article 3. "Data Processing" refers to the collection, storage, processing, transfer, provision, or publication of data.

[3] "Personal Information" is defined in the PRC Personal Information Protection Law, Article 4, as electronic or nonelectronic information that identifies or is able to identify a natural person.

3 Min Read

Author

Jacob Harding

Related Topics

IPO | Regulatory | Asia | Cyber Security

Related Capabilities

Transactions

Related Regions

Asia