July 23, 2021

China Plans Cybersecurity Review for Tech Companies Listing Abroad

Attorneys
Peng Yu
Oliver Nip
David Chen
Boxin Wang

On July 10, 2021, the Cyberspace Administration of China ("**CAC**"), China's top cyberspace regulator, published for public comment proposed amendments to existing Measures for Cybersecurity Review ("**Cybersecurity Review Measures**"), which have been in effect since June 1, 2020. The public comment period will continue until July 25, 2021.

In this alert, we focus on the proposed changes to the Cybersecurity Review Measures, which could impact how foreign investors exit from their investments in Chinese companies by way of initial public offerings ("**IPOs**") in foreign capital markets and how they may think about their future investments in Chinese companies.

Existing Offshore Financing and IPO Practices of Chinese Companies

For decades, foreign investors have invested in Chinese companies using a "red-chip" structure ("**Red-Chip Companies**"). A typical "red-chip" structure involves a string of offshore holding vehicles – typically an exempted company incorporated in the Cayman Islands (or less often, the British Virgin Islands) – holding 100% ownership of an onshore Chinese company, which operates the business in China. In some cases, especially where there are foreign investment restrictions under Chinese laws and regulations, a "red-chip" structure may be coupled with a variable interest entity ("**VIE**") structure, which involves using contractual arrangements – typically between a wholly owned enterprise established and controlled by one of the offshore holding companies and the onshore Chinese operating entity with shareholders that are exclusively Chinese nationals – to control and receive the economic benefits of the onshore Chinese operating entity. The "red-chip" structure coupled with the VIE structure has been used extensively to facilitate offshore financing of Chinese businesses in the technology, media, and telecommunications ("**TMT**") and Internet sectors, as well as in certain other regulated industries.

Up until now, for Red-Chip Companies, approval from the China Securities Regulatory Commission ("**CSRC**") and other Chinese regulators for overseas IPOs has not been required. Since the IPOs of Sina Corp., Netease and Sohu.com – the first Red-Chip Companies to complete overseas IPOs – on U.S. stock exchanges in the early 2000s, hundreds of Red-Chip Companies have completed overseas IPOs – typically in Hong Kong and the U.S. – to provide liquidity to their foreign and other investors and a relatively easy way to exit their investments.

"Foreign Country" Listings of Chinese Companies Targeted for Cybersecurity Review

In recent weeks, the Chinese government has signaled that it plans to regulate more strictly "foreign country" IPOs by Chinese companies. This shift is likely in response to increasing pressure in recent years from U.S. lawmakers and regulators to require additional information disclosures from U.S.-listed Chinese companies, which have stoked fears in China that U.S.-listed Chinese companies could be forced to disclose information and data about their businesses and users to the U.S. regulators that the Chinese government views as sensitive or that are of national security importance.

As a result, several items contained in the proposed amendments to the Cybersecurity Review Measures specifically target "foreign country" IPOs of Chinese companies. These include:

- A new requirement that critical information infrastructure operators and data processors who have personal information of more than one million users and are seeking IPOs in "foreign countries" like the U.S. must apply to the Cybersecurity Review Office, an interagency organization led by CAC, for a cybersecurity review ("**IPO Cybersecurity Review**"). For most Red-Chip Companies in the TMT and Internet sectors seeking "foreign country" IPOs, the threshold of having personal information of more than one million users is easily met.

- A new requirement that "IPO materials to be submitted" (e.g., draft registration statements or prospectuses) be submitted to the Cybersecurity Review Office for review as part of the IPO Cybersecurity Review. The proposed amendments do not explicitly specify when the IPO materials should be submitted to the Cybersecurity Review Office for review. However, the term "IPO materials to be submitted" used in the proposed amendments suggests that IPO materials should be submitted to the Cybersecurity Review Office for review *prior to* such materials being filed with foreign stock exchanges. One key practical issue that remains to be seen is whether and how the IPO Cybersecurity Review process can fit into the typical IPO process, e.g., whether both processes can proceed in parallel, or the relevant Chinese companies must obtain the cybersecurity clearance from the Cybersecurity Review Office before they can make IPO applications to foreign stock exchanges.

- The addition of CSRC as a new member agency responsible for the IPO Cybersecurity Review. While CSRC approval is not separately required, it is expected that the views of CSRC will be taken into account as part of the IPO Cybersecurity Review process.

- The expansion of the scope of cybersecurity review to include an assessment of national security risks that may arise from "foreign country" IPOs, including (i) the risk of core data, important data, or a large amount of personal information being stolen, leaked, destroyed, illegally used, or being exported out of China, and (ii) the risk of critical information infrastructure, core data, important data or a large amount of personal information being affected, controlled, or maliciously used by foreign governments after "foreign country" IPOs.

The proposed new requirement for Chinese companies to submit for IPO Cybersecurity Review would create uncertainty and risk of delay for their "foreign country" IPOs. Under the proposed amendments, the IPO Cybersecurity Review can take up to 70 business days for a general review and up to six months in aggregate if a special review is required. It is also possible that a Chinese company would not be able to pass the IPO Cybersecurity Review, which would effectively preclude its ability to complete its "foreign country" IPO.

However, notably, Hong Kong IPOs appear to be exempted. Although the proposed amendments to the Cybersecurity Review Measures do not include an explicit exemption for Hong Kong IPOs, most practitioners interpret the phrase "foreign country" IPOs to not include Hong Kong IPOs on the basis that Hong Kong is part of China as a sovereignty matter. If Hong Kong IPOs are exempted, it is expected that Red-Chip Companies in the TMT and Internet sectors will increasingly look to pursue their IPOs in Hong Kong instead of in the U.S. so long as they can meet the generally higher listing requirements of The Stock Exchange of Hong Kong ("**HKSE**"). However, for Chinese companies who cannot meet the listing requirements of HKSE (including revenue and profit requirements), their investors may face exit challenges. Furthermore, for Chinese companies that have adopted a VIE structure, they will need to comply with HKSE's guidance regarding the VIE structure, which requires the VIE structure to be used only to the extent necessary to address any limits on foreign ownership under the applicable Chinese laws and regulations, among other restrictions.

What to Expect

Even though the proposed amendments have not been finalized, the market response has been swift. Already, certain high-profile Red-Chip Companies have promptly announced that they are halting their U.S. IPO plans. If the proposed amendments come into effect as proposed, their impact on foreign investors and Chinese companies looking to access foreign capital markets is expected to be far-reaching, and they are likely to disrupt the market norm for overseas financing and listings by Chinese companies that has existed for decades.