Legal Commentary

January 5, 2022

HAN KUN
汉坤律师事务所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Preliminary Analysis of the Measures for Cybersecurity Review

Authors: Han Kun Law Offices Kevin DUAN | Kemeng CAI | Minzhe HU
Han Kun's Hong Kong Associated Law Firm Charles WU

On January 4, 2022, 13 ministries and commissions, including the Cyberspace Administration of China ("**CAC**") and the China Securities Regulatory Commission ("**CSRC**"), jointly promulgated the Final Measures for Cybersecurity Review (the "**Final Measures**"). The Final Measures are binding and will become effective on February 15, 2022. Overall, the Final Measures follow the basic regulatory framework set out in the Measures for Cybersecurity Review (Revised Draft for Comments) (the "**Draft Measures**") promulgated by such 13 ministries and commissions on July 10, 2021 (for our previous analysis on the Draft Measures, please click *here*). The Final Measures do contain, however, a few key revisions compared to the Draft Measures. This newsletter will briefly analyze these new revisions. We have also attached a comparison between the Final Measures and the Draft Measures for your reference.

The continued use of "listing in a foreign country", which may indicate regulatory intention to exclude operators listing in Hong Kong from the obligation of applying for a mandatory cybersecurity review

The concept of "listing in a foreign country" is retained in the Final Measures, though not further clarified. However, whereas the Regulations on Network Data Security Management (Draft for Comment) issued by CAC on November 14, 2021 (the "**Draft Regulations**") makes a distinction between the standards for a mandatory cybersecurity review for "listing in Hong Kong" and a "listing in a foreign country", the fact that the Final Measures apply the obligation for a mandatory cybersecurity review only to "listing in a foreign country" seems to indicate that the Final Measures intend to exclude Hong Kong listings altogether from mandatory cybersecurity reviews, though this interpretation has yet to be confirmed by regulators in practice. In addition, the Final Measures, prior measures and the Draft Measures all grant regulators the right to initiate cybersecurity reviews ex officio. Therefore, in practice, companies intending to list in Hong Kong may want to voluntarily apply for a cybersecurity review as a precautionary measure if they engage in a substantial amount of sensitive data processing activities. As with the Draft Measures, the Final Measures require CAC to respond within ten business days following the receipt of an application for cybersecurity review on whether there is a need for such review.

Like the Draft Measures, the Final Measures do not specify their scope based on the method of listing. The Final Measures only state that they apply to "application materials for listing such as an IPO". However, we are still inclined to believe that aside from traditional IPOs, Chinese companies proposing to list in the U.S. via SPACs (Special Purpose Acquisition Companies), RTO (Reverse Takeovers), direct listings and other methods should proactively apply for a cybersecurity review.

Entities subject to cybersecurity reviews when listing in a foreign country changed to "online platform operators"

The Final Measures stipulate that "online platform operators listing in a foreign country with more than one million users' personal information data must apply for a cybersecurity review with the Cybersecurity Review Office." This provision continues to follow the jurisdictional (i.e. "listing in a foreign country") and quantitative (i.e. one million users) cybersecurity review thresholds set out by the Draft Measures. However, entities subject to cybersecurity reviews have changed from "data processors" to "online platform operators". The Final Measures do not define "online platform operator", but the Draft Regulations defined it as "data processors who provide Internet platform services such as information publishing, social networking, transaction, payment, or audio-visual services". Common sense suggests that the scope of "online platform operators" seems narrower than "data processors" previously used and seems to exclude self-operated e-commerce services of fast-moving consumer goods companies that do not provide online platform services. However, the vagueness of "online platform operators" leaves room for interpretation by regulators in practice, who may require all types of operators with "more than one million users' personal information" to proactively apply for cybersecurity reviews.

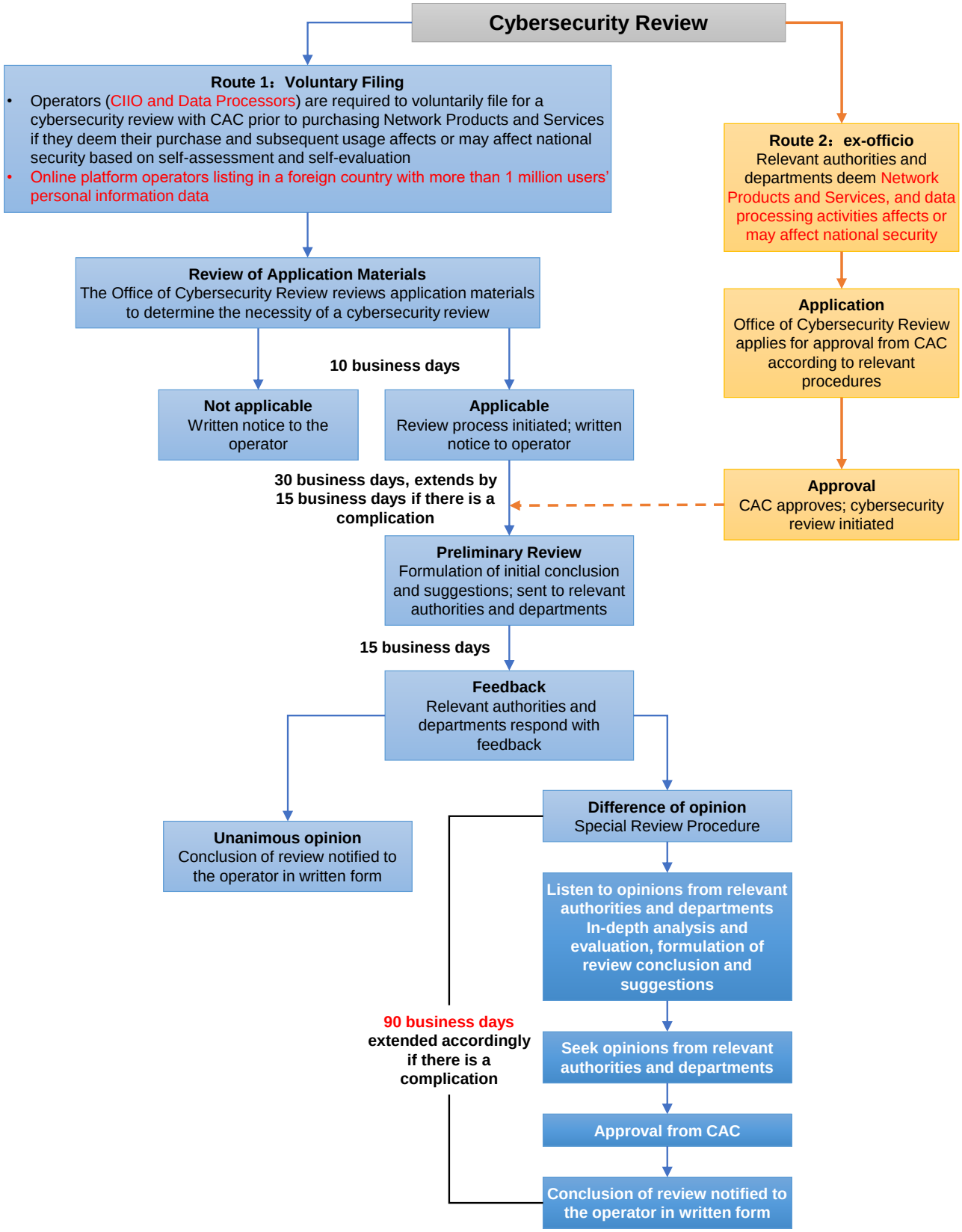
Timing and potential outcomes of a cybersecurity review

According to a Q&A on the Final Measures, online platform operators possessing personal information of no less than 1 million users are required to apply for a cybersecurity review prior to the submission of their listing application with non-PRC securities regulators. The outcome of the application may include: (i) review not required; (ii) where a review is initiated, the review concludes that the listing does not affect national security and grants clearance for the listing in a foreign country; and (iii) where a review is initiated, the review concludes that the listing does affect national security and the listing in a foreign country is prohibited. Operators with the former two outcomes may continue their listing application with non-PRC securities regulators. However, note that according to the Measures for the Overseas Issuance of Securities and Listing Record-Filings by Domestic Enterprises (Draft for Comments) issued by the CSRC on December 24, 2021, these companies must complete a separate filing procedure (of which clearance from CAC is a part) within 3 business days after the submission of their filing application.

Further extension of the time limit for special review procedures

Taken as a whole, the review process set forth in the Final Measures follows that of the existing measures and the Draft Measures with one exception: where there is disagreement between the members of the cybersecurity review group and the relevant departments, there will be a special review process seeking the opinions of the relevant authorities and the case will be reported to CAC. The time limit for this special

review procedure is extended to 90 business days from the 3 months stipulated in the Draft Measures, and this time limit may be extended accordingly to the extent there are complications. The overall review process according to the Final Measures is shown in the figure below.



Risk prevention and mitigation measures should be taken accordingly during the review period

Article 16 of the Final Measures states that "to prevent risks, the party should take risk prevention and mitigation measures during the review period in accordance with cybersecurity review requirements". Past practice suggests that "risk prevention and mitigation measures" may include suspending new-user registrations, suspending app downloads, etc., and may include actions like divesting relevant data assets or even suspending relevant online product services.

Formal launch of review hotlines concurrent with the publication of review application procedures

The Q&A accompanying the release of the Final Measures published the channels through which applications are reviewed and accepted. Namely, "the Cybersecurity Review Office is located within CAC. Specific work will be carried out by the China Cybersecurity Review Technology and Certification Center ("**CCRC**"). Under the guidance and leadership of CAC, CCRC will be responsible for tasks such as accepting and formally reviewing application materials. CCRC has also set up cybersecurity review consultation hotlines." We hope that CAC and the CCRC will publish as soon as possible clearer application guidelines for companies fulfilling their application obligations as soon as possible.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com

Kemeng CAI

Tel: +86 10 8516 4289
Email: kemeng.cai@hankunlaw.com

Charles WU

Tel: +852 2820 5617
Email: charles.wu@hankunlaw.com