LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

March 4, 2022 | Number 2934

China Issues New Rules on Cybersecurity Review for Network Platform Operators Listing Abroad

Under the new rules Chinese NPOs holding more than 1 million individuals' personal information must apply for a cybersecurity review prior to listing abroad.

Key Points:

- Chinese network platform operators (NPOs) holding personal information of more than 1 million users must apply for a cybersecurity review from the Cyberspace Administration of China (CAC) before being "publicly listed abroad." Draft guidance issued by the Chinese authorities also echo this cybersecurity review / data security assessment requirement.
- The CAC can initiate a cybersecurity review, presumably against any entity, if it deems that the entity's data processing activities or products and services will or may affect national security.
- The cybersecurity review may take 70 working days or, in exceptional cases, 160 working days or even longer.
- NPOs that plan to list in Hong Kong are unlikely to be required to apply for a cybersecurity review.

Background

On February 15, 2022, the Cybersecurity Review Measures (2021) (CRM 2021, unofficial English text available here) took effect. CRM 2021 was promulgated on December 28, 2021, by the CAC and 12 other Chinese central authorities, including the Ministry of State Security, the Ministry of Industry and Information Technology (MIIT), and the China Securities Regulatory Commission (CSRC). The CAC published the first draft of CRM 2021 on July 10, 2021, for public comments, and published the final version on January 4, 2022. The CAC cites the Data Security Law (DSL) as the legal basis for the authority of CRM 2021.

CRM 2021 replaced an earlier version of the Cybersecurity Review Measures, which was published in April 2020 and took effect in June 2020 (CRM 2020, unofficial English text available here). The key difference between CRM 2021 and CRM 2020 is that CRM 2021 expands the scope of entities subject to the cybersecurity review obligation to include "NPOs holding personal information of more than 1 million users applying for a public listing abroad." This expansion, which reveals that the Chinese authorities view foreign listings as a key risk from a cybersecurity perspective, has already impacted Chinese companies that wish to list abroad by limiting their choices.

Application Scope

CRM 2021 provides that entities that satisfy any of the following must apply for a cybersecurity review from the CAC:

- A critical information infrastructure operator (CIIO) that purchases network products and services that affect or may affect national security;
- An NPO that carries out data processing activities that affect or may affect national security; or
- An NPO that holds the personal information of more than 1 million individuals and proposes to be publicly listed abroad (this requirement is a new addition to CRM 2021).

According to CRM 2021, "network products and services" refers to core network equipment, important communications equipment, high-performance computers and servers, mass storage equipment, large-scale databases, application software, and cloud computing services, as well as other network products and services that have a major impact on critical information infrastructure security, cybersecurity, or data security. "Data processing" is defined under the DSL as the collection, storage, use, processing, transmission, provision, and disclosure of data.

Network Platform Operators

CRM 2021 does not define NPOs. According to the Draft Administrative Measures on Network Data Security Review (Draft NDSR, unofficial English text available here) released by the CAC for public comments on November 14, 2021, "Internet platform operators" are data processors that provide users with information distribution, social, transaction, payment, audiovisual, and other internet platform services. The draft Guidance for the Implementation of Subject Responsibility of Internet Platforms published by the State Administration for Market Regulation (SAMR) in October 2021 defines "platform operators" as entities that provide business premises, transaction aggregation, information dissemination, and other internet platform services to natural persons, entities, and other market entities.

Based on the above draft guidance, an NPO should be similar to internet platform operators / service providers. However, it is unclear (and this has not been explained in either CRM 2021, the Draft NDSR or other regulatory guidance) whether NPOs should be widely interpreted to include foreign companies that operate an internet platform business in China or operate an internet platform service that is available in China, rather than only NPOs which are Chinese incorporated companies / companies based or headquartered in China. Based on the intent of Chinese regulators to include foreign companies in its regulatory scope, which we can see in the extra-territorial application of the DSL and PIPL for example, it is likely that the former expansive interpretation will be taken by the CAC and foreign companies which qualify as an NPO will be subject to CRM 2021.

Some commentators are of the view that the level of national security risk involving foreign listed companies is mainly determined by the volume of data held by the company rather than the business model (e.g., an entity that operates an online platform), and therefore "network platform operators" should be interpreted expansively to include all operators that process data for the provision of internet services.[1] On the other hand, other commentators have pointed out that the addition of "network platform" to the term "NPO" in the final text of CRM 2021 (in contrast with the initial draft CRM 2021 published in July 2021, which only used the term "operators") suggests that the Chinese authorities intend to limit the scope of entities subject to a cybersecurity review to only NPOs rather than all "operators."

NPOs Listing Abroad in Hong Kong vs. Other Jurisdictions

CRM 2021 uses the term "publicly listed abroad," which is undefined, but the mandatory cybersecurity review is generally interpreted as not applicable to a Hong Kong listing, since Hong Kong is usually not considered as "abroad" under Chinese laws and draft regulations.[2]

For example, this concept of "publicly listed abroad" is reflected in the Draft NDSR, which divides overseas listings into two scenarios:

- Data processors handling the personal information of more than 1 million individuals that go public abroad; and

- Data processors that go public in Hong Kong, which affect or may affect national security.

Commentators generally see these signals as the Chinese government favoring Hong Kong listings over US listings. However, since the Draft NDSR and other current laws and (draft) regulations do not clearly define what "affect or may affect national security" means, companies that qualify as NPOs will likely still have to voluntarily apply for cybersecurity review (or at least informally consult and confirm with the Chinese authorities that one is not needed) before publicly listing in Hong Kong as a matter of prudence, thus weakening the advantage of listing in Hong Kong.[3] Importantly, the exclusion of Hong Kong from other overseas listing destinations is not confirmed in CRM 2021 and still remains subject to interpretation of the Chinese authorities; otherwise, the Chinese authorities could have adopted the language in the Draft NDSR for CRM 2021.

CRM 2021, without specifically so stating, grants the CAC the discretion to start a cybersecurity review, presumably against any entity, if it considers its products and services or data processing activities will or may affect national security. Therefore, Chinese companies listing in Hong Kong possibly will have to file for a cybersecurity review if the CAC deems the proposed listing could impact national security. Similarly, NPOs could be subject to a cybersecurity review if the CAC deems that their data processing activities could affect national security, even if they are processing personal information below the volume threshold (i.e., the personal information of more than 1 million individuals).

Other Issues for Publicly Listed Companies Abroad

CRM 2021 does not specify the types of public listings that are captured by "publicly listed abroad" and subject to a cybersecurity review, such as initial public offerings (IPOs), special purpose acquisition companies (SPACs), direct or indirect listings, listings through a variable interest entity (VIE), or reverse takeover. Therefore, if broadly interpreted, all forms of public listing abroad could be subject to a mandatory cybersecurity review if the 1 million threshold is met.

Another issue that remains unresolved is whether CRM 2021 applies retrospectively, i.e., whether NPOs that are already listed in Hong Kong or abroad are required to retroactively file for cybersecurity reviews with the CAC. Some commentators have argued that, based on a literal interpretation, companies already listed abroad do not need to file for cybersecurity reviews because the term used is "are to be publicly listed abroad" rather than, for example, "companies that are publicly listed abroad." However, a mandatory cybersecurity review may still be required if an already listed company abroad issues additional shares or bonds that may involve national security risks, which may trigger scrutiny from the Chinese authorities from a national security perspective.

Factors Contributing to the Cybersecurity Review

According to CRM 2021, the cybersecurity review shall focus on the assessment of the following national security risk factors:

1. Risks of illegal control, interference, or destruction of critical infrastructure (CII) caused by the use of products and services;

2. The harm to the business continuity of CII caused by interruptions in the supply of products and services;

3. The products' or services' security, openness, transparency, and diversity of sources of products and services, reliability of supply channels, and risks of supply interruption due to political, diplomatic, trade, or other factors;

4. Compliance with Chinese laws and regulations by product and service providers;

5. Risks of theft, disclosure, damage, illegal use, or cross-border transfer of core data, important data, or large amounts of personal information;

6. Risks of influence, control, or malicious use of CII, core data, important data, or large amounts of personal information by foreign governments, or cybersecurity risk caused by foreign listing; and

7. Other factors that may endanger CII security and national data security.

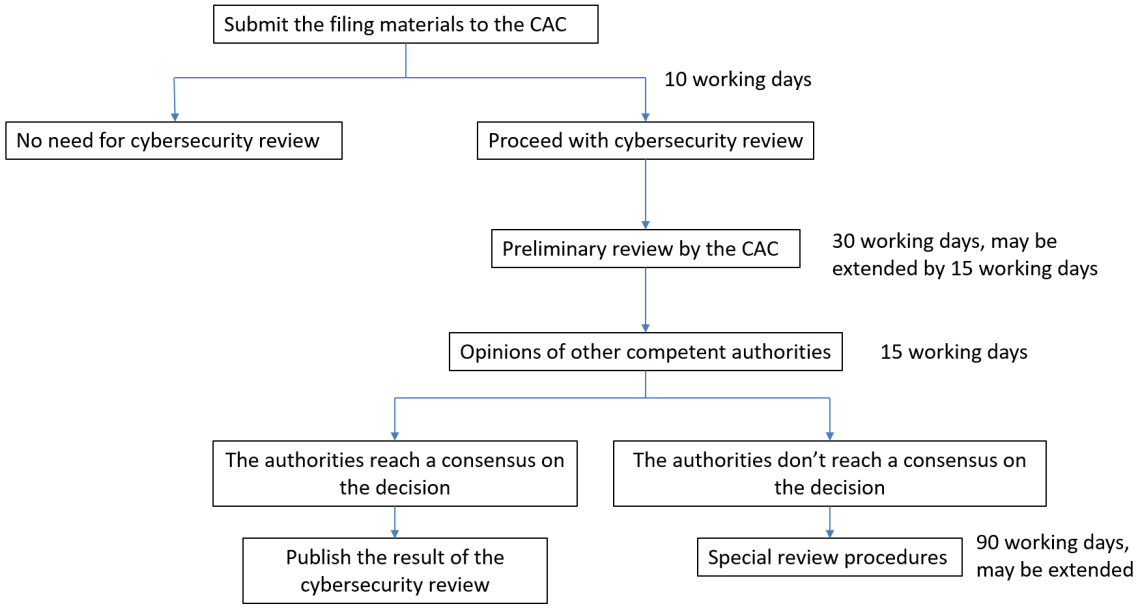
"Important data"[4] is a concept which was first introduced in the CSL and further explored in the DSL. Although it still remains undefined under the CSL and DSL, regulatory guidance suggests it refers to data collected or derived in the PRC that closely relates to national security. See Latham's Client Alert on the DSL for a detailed discussion on the collection and storage of important data.

Among these factors, the risk of "influence, control or malicious use by foreign governments" is newly added compared to CRM 2020. This factor underpins the expansion of CRM 2021 to include NPOs that plan to list abroad. By way of background, the US Securities and Exchange Commission (SEC) adopted rules implementing the Holding Foreign Company Accountable Act (HFCAA) on December 2, 2021, requiring foreign companies listed in the US to file documents with the SEC certifying that the company is not owned or controlled by a foreign government, and requiring these companies to comply with the audit standards of the Public Company Accounting Oversight Board (PCAOB). Under the HFCAA, US-listed companies may face delisting if they fail to provide the PCAOB with an audit primer within a specified timeframe.

Commentators generally believe that the CRM 2021 provisions regarding foreign government risk are in large part responding to the HFCAA, i.e., to prevent data security risks arising from information being provided to foreign regulators by Chinese companies during the listing process abroad.[5] How the economic needs of Chinese companies seeking financing overseas will be balanced with the national security concerns of the Chinese authorities in light of the mandatory cybersecurity review requirement under CRM 2021 remains to be seen.

Procedures and Timing

CRM 2021 sets out the below procedures for cybersecurity review:



An NPO can expect three possible outcomes after it applies for a cybersecurity review in respect of its proposed public listing abroad:

1. The CAC determines that a cybersecurity review is not needed;

2. The CAC determines that a cybersecurity review is needed and, once the review is completed, finds no national security concern and the NPO can proceed with the public listing abroad; or

3. The CAC determines that a cybersecurity review is needed, and once the review is completed, decides that there is a national security concern and the NPO may not proceed with the public listing abroad.

Documents for Cybersecurity Review

Companies required by CRM 2021 to apply for a cybersecurity review shall submit the following materials to the CAC:

- Application letter;

- Analysis report on the impact or potential impact on national security;

- Application documents for listing, such as purchasing documents, agreements, contracts to be executed, or the proposed IPO; and

- Other materials as required by the authorities for their cybersecurity review.

The CAC has not yet published any template for or guidance on the application letter or national security impact analysis report. This may impact the timeframe for future foreign listings of Chinese companies as companies will first need to prepare their listing application materials for cybersecurity review in China. As a result, Chinese companies will likely need to obtain a decision on cybersecurity review before they can submit their listing applications to foreign listing regulators, which can take a long time. It is not clear whether the listing application materials can be modified during this period.

Timeline

- **Shortest possible processing time:** As shown in the flowchart above, if the various competent authorities involved in the cybersecurity review are able to reach a consensus on the decision, the time span from the submission of application materials to the publication of the decision is 55 working days (extendable by 15 working days).

- **Longest possible processing time:** If the authorities are unable to reach a consensus, a special review of 90 days will be added (i.e., 55 + 15 + 90 = 160 working days), and a special review can be extended with no cap. Additionally, if the Chinese authorities request supplementary materials, the time needed to produce such materials does not count towards the review timeline, which is paused until such materials are provided. The timeline would then be unpredictable.

Notably, according to a CAC press release, NPOs should apply for the cybersecurity review prior to filing the foreign listing application with the relevant foreign listing regulator. During the cybersecurity review process, the review opinions of competent authorities will be obtained. Next, according to the draft Administrative Measures for the Filing of Foreign Securities Offerings and Listings by Domestic Enterprises, issued by the CSRC on December 24, 2021 (CSRC Draft Measures), Chinese issuers should submit the outcomes of such cybersecurity review, including the review opinions of competent authorities, to the CSRC within three working days after the application documents for the foreign listing have been submitted to the foreign listing regulator. If the cybersecurity review filing requirements under the CSRC Draft Measures take effect, then the period for foreign listings of Chinese companies will be further extended.

Other Obligations on Overseas Listed Companies

Annual Data Security Assessment and Reporting

The Draft NDSR provides further guidance on the legal requirements underpinning the Cybersecurity Law (CSL), the DSL, and the Personal Information Protection Law (PIPL). It provides for far-reaching application and requires both data processors of important data (including those processing personal information of more than 1 million individuals) and data processors listing abroad to perform an annual data security assessment, either via self-assessment or by a qualified third party, and report the previous year's annual data security assessment results to the local CAC before January 31 of each year. The annual data security assessment should include all of the following:

- The processing of important data;

- Data security risks identified and disposal measures;

- Data security management system, data backup, encryption, access control, and other security protection measures, as well as the implementation of the management system and the effectiveness of protective measures;

- The implementation of data security laws, administrative regulations, and national standards;
- The occurrence of data security incidents and disposal;
- The security assessment of data sharing, trading, entrusted processing, and important cross-border data transfer;
- Data security-related complaints and handling; and
- Other data security issues specified by the CAC and competent authorities.

The Draft NDSR reinforces the view that the Chinese authorities view cybersecurity as a key risk and an area of focus — although importantly it still remains in draft form with no clear effective date.

Declaration and Reporting Obligations Under Restructuring

The Draft NDSR also imposes declaration and reporting obligations on internet platform operators and data processors undergoing a merger, reorganization, or separation (collectively, restructuring) under the two following scenarios:

- Internet platform operators that hold large amounts of data relating to national security, economic development, or public interests must apply for a cybersecurity review before restructuring or performing other activities that affect or may affect national security; and
- Data processors undergoing restructuring and process important data or personal information of more than 1 million individuals must report to the local competent authorities or the local CAC.

The Draft NDSR does not define what volume qualifies as holding "large amounts of data."

Notably, the Draft NDSR does not specify the consequences if an internet platform operator fails to pass or complete the cybersecurity review. Presumably, like one of the possible outcomes under CRM 2021 (see flowchart above), a failed result means the operator may not proceed with the proposed restructuring; however, this presumption is yet to be confirmed since the Draft NDSR is still in draft form.

Since restructuring often occurs in the course of a Chinese company's overseas listing, the reporting obligation may easily be triggered. The Draft NDSR does not provide a clear definition of merger, reorganization, or separation, and does not explain whether it covers such changes in overseas company structures. However, commentators generally understand that any form of reorganization of overseas listing structures are likely to fall within the scope of application of this provision.[6]

Finally, the Draft NDSR requires large internet platform operators to report to the CAC and industry regulators when setting up headquarters, operation centers, or R&D centers outside mainland China. According to the draft Guide of Classification and Grading of Internet Platforms published by the SAMR on October 29, 2021, a "large Internet platform" is one that (1) has a minimum of 50 million active users in China in the previous year, (2) has a market capitalization (valuation) of a minimum of CNY 100 billion at the end of the previous year, and (3) has an outstanding performance in the main business and a strong ability to limit merchants' access to consumers (users).

Cross-Border Data Transfer Security Assessment

On October 29, 2021, the CAC released a draft Regulation on Cross-Border Data Transfer Security Assessment (Draft CBDTSA), which aims to clarify the data export requirements under the CSL, DSL, and PIPL. According to the Draft CBDTSA, entities undertaking the following activities must pass a cross-border data transfer security assessment organized by the CAC:

- Cross-border transfer of important data and personal information collected and generated by CIIOs;
- Cross-border transfer of important data;
- Cross-border transfer of personal information by a personal information processor that has cumulatively *processed* the personal information of more than 1 million individuals (the language in the Draft CBDTSA seems to suggest that *any* cross-border transfers by such a personal information processor will be subject to a cross-border data transfer security assessment, however this has not been further clarified or confirmed by the CAC);
- Cumulatively *transferring* the personal information of more than 100,000 individuals abroad; or
- Cumulatively *transferring* the sensitive personal information of more than 10,000 individuals.

Although the Draft CBDTSA is still in draft form, the volume thresholds helpfully clarify when personal information processors are required to pass a mandatory security assessment by the CAC prior to a cross-border data transfer under the PIPL. Overseas listed companies, especially internet platform operators, are likely to easily meet one of the criteria and trigger the cross-border data transfer security assessment requirement as data will likely be accessed or transferred overseas on a regular basis.

Notably, even though the same regulator (the CAC) leads both the cybersecurity review under CRM 2021 and the cross-border data transfer security assessment under the Draft CBDTSA, the scope, aims, and considerations of the two assessments are distinct from one another. Therefore, an entity may be subject to both review and assessment, e.g., an NPO with more than 1 million individuals' personal information that seeks to list abroad and wishes to transfer personal information outside of China as part of the listing application.[7]

Key Takeaways

The promulgation of CRM 2021 marks a step forward in China's strict regulation of Chinese companies' overseas listing and adds another hurdle to companies' listing process. However, as the CSRC has repeatedly emphasized to the media, the Chinese government has no intention of banning Chinese companies from listing overseas, but rather wants to strengthen regulation from a national security and data security perspective. Going forward, Chinese companies will need to focus on the following issues when considering an overseas listing:

- **Choice of overseas listing destination:** Most commentators tend to believe that Hong Kong listings are not subject to mandatory cybersecurity review, which would give Hong Kong listings an advantage over US listings, but companies will still need to pay close attention to China's future policy and market practice trends.
- **Whether a cybersecurity review is required:** The threshold of "holding personal information of more than one million individuals" under CRM 2021 may be easily reached for many Chinese

companies seeking an overseas listing, and even if the issuer is not a typical NPO, the possibility of a cybersecurity review filing cannot be ruled out.

- **Timeline for overseas listings:** Under CRM 2021, companies will need to prepare their listing application documents prior to the cybersecurity review filing and obtain the cybersecurity review conclusions before submitting the listing application to the foreign regulator. This process can take 70 working days, or in exceptional cases, 160 working days or even longer. The window for an overseas listing can be very short for companies, so the impact of the cybersecurity review in terms of timing must be taken into account.

- **Other obligations:** Besides CRM 2021, the Draft NDSR and Draft CBDTSA will impose additional obligations on overseas listing companies once they come into effect. While these obligations are not formalized yet (since they are still in draft form), companies that intend to list overseas should pay close attention to relevant legislation and practical developments.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Hui Xu
hui.xu@lw.com
+86.10.5965.7023
Beijing

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

Bianca Lee
bianca.lee@lw.com
+852.2912.2781
Hong Kong

This Client Alert was prepared with the assistance of foreign legal consultant Zurui Yang in the Beijing office of Latham & Watkins.

You Might Also Be Interested In

China's New Data Security Law: What to Know

China Issues Draft Data Security Law for Public Comment

Extensive Changes to Singapore's Data Protection Regime Take Effect

Hong Kong Considers Sweeping Changes to Privacy Laws

Endnotes

1 Zhong Lun Law Firm, *Cybersecurity Review Measures Settled: What's the Impact on Overseas Listing*, January 10, 2021. See http://www.zhonglun.com/Content/2022/01-10/1608191725.html.

2 See, for example, Fangda Partners, *China's Cybersecurity Review Enters a New Phase: How to Read the New Changes in the Cybersecurity Review Measures*, January 5, 2021. See https://law.wkinfo.com.cn/professional-articles/detail/NjAwMDAxNTE0MDE%3D?q=%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E5%AE%A1%E6%9F%A5%E5%8A%9E%E6%B3%95.

3 Han Kun Law Offices, *A Brief Comment on the Impact of the Draft Administrative Regulation on Network Data Security to Overseas Listing of Companies*, November 15, 2021. See https://www.hankunlaw.com/downloadfile/newsAndInsights/0d67723eabd5186cb98e34cd677acdbd.pdf.

4 The term "important data" was first introduced in the 2016 in the CSL, which did not provide a definition. Under the 2017 draft recommended national standard "Guidelines for Cross-Border Data Transfer Security Assessments" (the Draft Guidelines), "important data" refers to data collected or derived in the PRC that closely relates to national security, economic development, and public interests. Appendix A of the Draft Guidelines sets out a detailed list of "important data" in various industries. For example, in military sector, "important data" include information on the name, quantity, source and agent of purchased components, software, materials, industrial control equipment test instruments, and information on the internal name, geographical location, construction plans, security planning, secrecy level, plant drawings, storage volume, reserves of military research and production institutions; in petrochemicals sector, "important data" include main economic and technical indicators and major policy measures in annual, medium-term and long-term development plans of the national petroleum and petrochemical industries, and annual import plans for important production materials in petrochemical industry.

5 De Heng Law Offices, *Read the Cybersecurity Review Measures from the Perspective of Overseas Listing*, January 8, 2021. See https://new.qq.com/omn/20220108/20220108A047FT00.html.

6 *Supra* note 3.

7 Supra note 2.