中倫律師事務所
ZHONG LUN LAW FIRM
北京市朝阳区金和东路 20 号院正大中心 3 号楼南塔 23-31 层，邮编：100020
23-31/F, South Tower of CP Center, 20 Jin He East Avenue, Chaoyang District, Beijing 100020, P. R. China
电话/Tel：+86 10 5957 2288　传真/Fax：+86 10 6568 1022/1838
网址：www.zhonglun.com

Introduction to Cybersecurity Review System in China

Rachel Li

Jason Jia

Megan Li

From Zhong Lun Law Firm

In July 2021, China's Cybersecurity Review Office ("**CRO**"), a subordinate office under the Cyberspace Administration of China ("**CAC**") responsible for coordinating the implementation of China's Cybersecurity Review System, announced that it had initiated cybersecurity reviews against four mobile applications operated by three Chinese companies. It was the first time that CRO made public announcements on cybersecurity reviews against companies since the *Measures for Cybersecurity Review* (the "**2020 Measures**") took effect on 1 June 2020.

Further to the announcements, on 10 July 2021, CAC issued the *Measures for Cybersecurity Review (Revised Exposure Draft)* (the "**2021 Exposure Draft**") to solicit public opinions. According to Article 6 of the 2021 Exposure Draft, operators who possess personal information of over a million users must apply for cybersecurity review before listing abroad. Besides, any procurement of network products by a Critical Information Infrastructure Operator ("**CIIO**"), or any data activities by data processors that affect or may affect national security ("**NS Data Processor**", together with CIIOs, hereinafter as "**Cybersecurity Review Targets**"), shall go through cybersecurity review in accordance with the provisions.

On 17 August 2021, the State Council of China announced that it had passed the *Regulation on the Security Protection of Critical Information Infrastructure* (the "**CII Regulation**"), which was formulated under the *Cybersecurity Law* ("**CSL**") to ensure the security of CII as well as maintain cybersecurity.

The *Data Security Law* ("**DSL**") came force as of 1 September 2021 shortly after the adoption of the *Personal Information Protection Law* ("**PIPL**") on 20 August 2021. Cybersecurity Review Targets may face a new era of data compliance scrutiny. This post provides a brief introduction to Cybersecurity Review Targets and Cybersecurity Review System under China's laws and regulations, explains Cybersecurity Review Targets' compliance obligations in the procurement and running of CII, and analyses the legal consequences for breach of cybersecurity laws and regulations, so as to provide more background information on recent enforcement actions regarding cybersecurity review initiated by the CAC.

Is your company a NS Data Processor?

The concept of "Data Processor" is not clearly defined in the 2021 Exposure Draft. We may examine its connotation in light of relevant provisions in other cybersecurity and data protection laws. Based on the DSL and the PIPL, "Data Processor" shall include the network operators who are engaged in the collection, storage, use, processing, transmission, provision, trading and publication of data. Compared to CIIO, no prior approval from the relevant authorities will be imposed on Data Processors that cover a wide range of objects.

Is your company a CIIO?

"Critical Information Infrastructure Operators", or CIIOs, means the operators of information infrastructure in important industries and sectors (such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs), the disruption, destruction or data leakage of which could result in catastrophic and far-reaching damage to the national security, the economy, social well-being and public interests. Both domestic and foreign-invested companies can be CIIOs.

In accordance with Article 9 of CII Regulation, the CII protection departments will formulate detailed rules for the accreditation of CII. Currently, based on Article 31 of the CSL and Article 2 of CII Regulation, a company can preliminarily evaluate whether its network system constitutes a CII and thus the company will be classified as a CIIO by asking the following questions:

Q1: Is your company in an important industry/sector?

- Is your company in any of the important sectors of public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs?

Q2: Will cybersecurity incidents of your company's network system wreak damage?

- Will it result in catastrophic and far-reaching damage to the national security, economic and social well-being and public interests, if your company's network system is destroyed, loses functions or encounters data leakage?

An affirmative answer to any of the above two questions means that your company may be classified as a CIIO. However, in regard to the scope of CII, the above two questions are far from exhaustive. CII may also cover other network infrastructure or information systems, the damage, malfunction or data leakage of which could severely harm the national security, the economy, people's livelihood and public interests.

Under the 2020 Measures, competent industry regulators have the power to accredit lists of CIIOs. In practice, though there have been no published lists of CIIOs yet, regulators of different industries have identified some companies as CIIOs.

What are Cybersecurity Review Targets' Compliance Obligations under Cybersecurity Review System?

1. What Is the Compliance Obligation under Cybersecurity Review System?

The CSL provides overarching principles and high-level requirements for CII compliance. Under the 2020 Measures, in line with the framework set out by the CSL, only CIIOs were required to apply for cybersecurity review by the CRO when procuring network products or services. This narrow application has been extended under the 2021 Exposure Draft to also include NS Data Processors' data processing activities that affect or may affect national security and/or its public listing abroad.

Under the 2021 Exposure Draft, Cybersecurity Review Targets shall be subject to cybersecurity review conducted and organized by the CRO under the following circumstances:

- Where CIIOs procure the network products or services which affect or may affect national security;
- Where Operators (including CIIOs and NS Data Processors) holding personal data of over a million users must apply for cybersecurity review before listing abroad;
- Where any department of cybersecurity review working mechanism is of the opinion that NS Data Processors' network products or services, data processing activities or their listing abroad affects or is likely to affect national security.

2. How is the Cybersecurity Review Procedure Triggered?

The review will be triggered under two pathways: (a) CIIOs and NS Data Processors applying for the review if they foresee any risk; and (b) the CAC initiating the review *ex officio.*

Pathway I: CIIOs and NS Data Processors applying for cybersecurity review

Cybersecurity Review Targets shall anticipate potential national security risks and report "risky purchase" to the CRO for cybersecurity review under the 2021 Exposure Draft, and the following application materials shall be submitted for review:

- The application form;
- An analytical report on whether national security is or may be affected;
- The purchase document/agreement, the contract to be executed, or the IPO materials to be filed;
- Other materials needed for cybersecurity review.

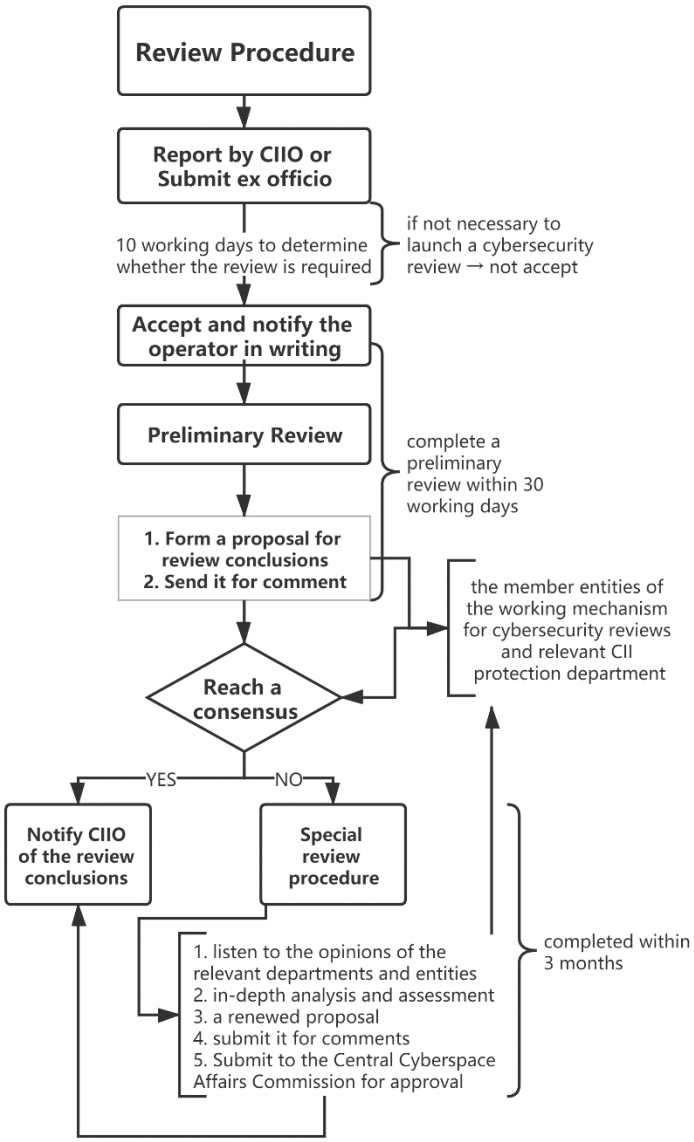
Besides, the CIIOs shall, through purchase documents and agreements, require product and service providers to cooperate with cybersecurity review under Article 6 of the Measures.

Pathway II: the CRO initiating the review *ex officio*

If a network product or service is deemed by the departments of cybersecurity review working mechanism to affect or potentially affect national security, the CRO shall submit it to the Central Cyberspace Affairs Commission for approval and conduct the review in accordance with the provisions of these Measures.

3. What is the Cybersecurity Review Procedure?

In accordance with the 2021 Exposure Draft, the whole procedure of cybersecurity review is as follows:



What Are Legal Consequences for Breach?

In terms of legal consequences of breaching cybersecurity review obligations, Article 20 of the 2021 Exposure Draft has cited the CSL and the DSL as the basis. According to the CSL, any Cybersecurity Review Target that fails in applying for cybersecurity review or uses any products and services banned in cybersecurity review would be subject to a fine up to 10 times of the price of the procured products or services, and a fine up to CNY 100,000 will be imposed on the responsible person. Besides, competent departments are authorized to order the business entity to cease its use of such products or services.

While according to the DSL, breach of data security obligations may lead to a maximum fine of

CNY 10 million in case of severe violations.

In practice, if competent departments believe that a company is not fulfilling its cybersecurity review obligations as a CIIO or a NS Data Processor, they may conduct investigations and assessments immediately and impose various penalties, which depend on the severity of the violation and may include administrative warnings, ordered rectification, and administrative fines. Once cybersecurity review is triggered, regulators may order app stores to remove the apps of such Cybersecurity Review Target or prohibit new user registrations for such apps. For example, under the orders of CAC, one ride-sharing app was removed from all the app stores in China and required to rectify the relevant problems, and new user registrations for other three apps were also suspended.

What Should Cybersecurity Review Targets Do in Operation to Meet the Compliance Obligations?

The 2021 Exposure Draft further enhances cybersecurity and data security supervision on the basis of the CSL and the DSL. The implementation of the measures will pose significant impacts on Cybersecurity Review Targets in China. Therefore, the companies that may be classified as Cybersecurity Review Targets should take these implications into account in daily operations and ramp up security and data protection compliance in order to meet the obligations under the CSL, the DSL and other relevant laws and regulations.

1. Procurement Compliance

Apart from CIIOs and NS Data Processors which are the direct targets of cybersecurity review, suppliers to these Cybersecurity Review Targets, i.e., companies which provide products and services, may also be affected by cybersecurity review. The 2021 Exposure Draft requires that Cybersecurity Review Targets shall, through the procurement documents and agreements, request the suppliers of products and services to cooperate in cybersecurity review, including to commit that it will not illegally acquire user data through products and services, or illegally control or manipulate user's equipment, and will not suspend the supply of products or necessary technical supporting services without reasonable cause. Considering the above, it's recommended that the parties should apply for cybersecurity review before signing the procurement contract, or they should specify in the contract that the contract will be effective only if the products or services pass the cybersecurity review.

2. MLPS Requirements

The system of Multi-level Protection for Cybersecurity ("**MLPS**") was formally established under the CSL. The *Regulations on Multi-level Protection for Cybersecurity (Exposure Draft)* issued by the Ministry of Public Security in 2018 and the series of national standards（"**MLPS 2.0**"）released thereafter specify detailed rules for the implementation of MLPS, which require the network operators to classify their information and network systems from Level 1 to Level 5 based on the impact on the national security, social order, public interests, the legitimate rights and interests of citizens, legal persons and other organizations if such systems destroyed, lost functions or encountered data leakage. The operators should implement various measures to improve their protection capacity and safeguard the security of their network and information depending on the

classification of the systems. More administrative procedures will be imposed if a system is classified as Level 2 or above.

Therefore, Cybersecurity Review Targets should positively perform the security protection obligations under MPLS 2.0, and conduct multi-level protection implementation, assessment and filing as required to manage cybersecurity risks and ensure the foundational cybersecurity compliance.

3. Data Categorization and Important Data Protection

The DSL provides that the government will establish a categorical and hierarchical system for data protection and publish an important data catalogue at the national level, and all local governments and governmental departments shall determine the catalogue of important data for their respective region and departments and for relevant industries and sectors, and conduct key protection of data included in the catalogue.

Therefore, Cybersecurity Review Targets processing such important data should comply with the following requirements:

- Designating responsible persons and data security management bodies to implement responsibilities for data security protection;
- Periodically carrying out risk assessments for the data processing activities and submitting risk assessment reports to the regulators.

4. Cross-border Data Transfer

Cybersecurity Review Targets should attach importance to the compliance of cross-border data transfer. Under the CSL and DSL, all personal data and important data collected or generated by CIIOs within the territory of China should be stored in China in principle. If a CIIO needs to transfer such data outside China, it should go through a security assessment approved by the competent authority. Furthermore, in accordance with the DSL, the government will further formulate relevant regulations on the cross-border transfer of important data by companies other than CIIOs. Despite the implementing rules to be further published by the government, it seems that even if companies are not classified as CIIOs, they may also be subject to restrictions on cross-border transfer if they process data that falls under the important data catalogues, which such companies should be pay attention to.

***