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 22-31 层，邮编：100020
22-31/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

China's Cybersecurity Review Regime: Framework and Latest Trends

Author: John Jiang, Scott Yu, Rachel Li, Daisy Xu

On 31 March 2023, the Cybersecurity Administration of China ("**CAC**") made a formal announcement[1] regarding the initiation of a cybersecurity review procedure aimed at scrutinizing the products distributed in China by Micron Technology Inc. ("**Micron**"). CAC's official statement explicitly clarifies that this review aims at preserving the supply chain security for critical information infrastructure ("**CII**") so to mitigate hidden risks and safeguard national security.

Over the recent years, China has undergone a rapid involvement in its legislative framework concerning cybersecurity and data security, accompanied by an uptick in relevant enforcement activities. The well-known cybersecurity review on Didi Chuxing, the Chinese counterpart of Uber, which had continued for approximately a year and ended up with *a US$1.2 billion fine* and a delisting of the company from Nasdaq, is the best showcase of how significant the consequence of a cybersecurity review in China could be. In this article we intend to provide a brief introduction of the Chinese legislative framework and its enforcement behind the cybersecurity review regime, along with its latest trends and implications.

I. Legal Basis of the Cybersecurity Review Regime

The concept of cybersecurity review was firstly introduced by the *Cybersecurity Law of the PRC* ("**CSL**"), which came into force on June 1 2017. According to article 35 of the CSL, a critical information infrastructure operator ("**CIIO**[2]") must apply and pass a security review co-organized by the CAC and other competent regulatory authorities before it purchases network products and/or services that may affect national security.

Aligning with the approach under CSL, *The Data Security Law of the PRC* ("**DSL**"), taking effect on Sep 1, 2021, further stipulates that competent authorities could carry out national security reviews to examine data processing activities that may impact national security. After that, CAC expanded the scope of the cybersecurity review regime to cover not only supply chain security of CIIOs but also data processing activities that may impact national security. In particular, cybersecurity review will be triggered when network platform operators that obtain personal information of more than one million individuals

[1] Regarding the official statement CAC issued, please refer to http://www.cac.gov.cn/2023-03/31/c_1681904291361295.htm.

[2] CIIOs refer to those entities operating critical information infrastructures that could have impact on national security and public interests. In practice, usually China competent industry regulator and/or local public security authority will approach the company who may fall into the CIIO category, carry out a series of identification measures and then issue an identification certificate or similar documents to identify the company as a CIIO.

seek for public listing at a foreign stock market.

In summary, China's cybersecurity review procedure mainly covers two purposes, one is to preserve the supply chain security of CIIOs, the other is to dig in data processing activities that may impact national security. For the investigation against Micron, CAC specified that the purpose was to preserve the supply chain security of CIIOs.

In addition to CSL and DSL, Chinese government also issued a few dozens of administrative regulations to implement the requirements under the laws, which together with the two laws, formed China's cybersecurity review regime.

II. Key Considerations of the Cybersecurity Review Procedure Focusing on Supply Chain Security of CIIOs

1. *Initiation of a Cybersecurity Review: Voluntary Filing vs. Regulator's Unilateral Action*

Cybersecurity review aiming to preserve supply chain security of CIIOs will be triggered in the following two scenarios:

- If an entity falls into CIIO, it may voluntarily apply to regulators for a cybersecurity review before its procurement of network product and service that affect or may potentially affect national security; or
- If competent regulatory authorities finds that any network product and service affects or may potentially affect national security, they may initiate cybersecurity review upon CAC's approval.

To date, the first scenario (i.e., CIIO's voluntary application for review) has accounted for the majority of the dozens of actual review cases in the past several years. The second scenario (i.e. reviews initiated by regulator) is rarely seen; actually, the Micron case is the first case where CAC proactively initiates a cybersecurity review procedure against a network product/service provider. It may signal that Chinese regulators started to be more active in taking action in securing supply chain security of CIIOs from cybersecurity perspective.

2. *Key Consideration Points in Review*

In a cybersecurity review procedure for purpose to preserve the supply chain security of CIIOs, the relevant authority will review and assess the following key points:

(1) Network product's and service's impacts to CII

- the risks of CII being illegally controlled, interfered with or damaged, and important data being stolen, leaked or destroyed, as a result of the use of products and services;
- the risks to the continuity of CII's business.

(2) Security and compliance status of the network product and service used by the CIIO

- security, openness and transparency of the product and service;
- whether the product and service are in full compliance with applicable Chinese laws and regulations.

(3) The supply chain stability of the network product and service used by the CIIO

- whether the supply of such product and service will be interpreted due to

political, diplomacy and/or other reasons.

(4) Other factors that may endanger the CII and/or national security.

*****

For further inquiries on cybersecurity and data compliance in China, please feel free to contact us:

Rachel LI Email: lirui@zhonglun.com Direct Line: (8610) 5957-2143	**Scott YU** Email: scottyu@zhonglun.com Direct Line: (8610) 5957-2078