COVINGTON

China Seeks Public Comments on Draft Regulation on Cybersecurity Review of Network Products and Services

February 7, 2017

Data Privacy and Cybersecurity

On February 4, 2017, the Cyberspace Administration of China ("CAC") released the draft Measures on the Security Review of Network Products and Services ("the draft Measures") for public comment (official Chinese version available here; Covington's translation of the draft Measures is here). The comment period ends on March 4, 2017.

The issuance of the draft Measures marks an important step toward implementing China's Cybersecurity Law, which was promulgated on November 7, 2016 and will take effect on June 1, 2017 (see the Covington alert on the new law here). This long-anticipated regulation offers more guidance on the security reviews mandated by Article 35 of the law, which requires operators of Critical Information Infrastructure ("CII") to ensure that any procured network products and services that may affect national security have passed a "national security review."

Although the draft Measures use the term "cybersecurity review" rather than "national security review," the review process in fact focuses on protecting China's national security in cyberspace. The draft Measures elaborate on the review's scope, substantive criteria, responsible agencies, and process.

While the draft Measures furnish some basic parameters of the review structure, the meaning and scope of many of the draft Measures' provisions are unclear. In particular, the draft Measures do not clearly address important procedural issues such as the potential timeframe for the review process and information needed to be submitted for the review.

Companies seeking to supply network products and services to operators of CII in China (which could also include multinationals operating in sectors such as transportation, energy, finance, and telecommunications in China) should be aware of this developing process. As the draft Measures come into force in the coming months, such companies will need to carefully assess the implications of the draft Measures, including whether to voluntarily seek security reviews for their products or services.

Background

Even before the enactment of the Cybersecurity Law, the government had mandated security reviews of network services procured by government agencies and organs of the Communist Party of China ("CPC"). Examples include cloud computing, information technology system design and development, and data processing services, among others. These reviews require suppliers to submit information on themselves and their services, as well as information on the testing or evaluation centers which certify the security of such services. In addition, some sector

regulators, such as the People's Bank of China ("PBOC") and the Ministry of Industry and Information Technologies ("MIIT"), have mentioned in various policy documents that security reviews should be conducted when companies in the regulated industries procure network products or services.

Article 35 of the Cybersecurity Law institutionalized the security review requirements across the board by mandating that operators of CII ensure that any procured network products and services that may affect national security have passed a "national security review." The draft Measures aim to implement this article.

Scope of Review

The draft Measures provide that "important network products and services" used by information systems that implicate national security and public welfare should pass a "cybersecurity review" (Article 2). The term "important network products and services" is not defined.

The document further clarifies that network products and services supplied to two types of entities should be subject to the review process:

- Government agencies, CPC organs, and entities in "key sectors" such as finance, telecommunication, and energy (Article 10); and
- Operators of CII, if the procurement "may affect China's national security" (Article 11).

These two provisions appear to create a two-tier system: government agencies, CPC organs, and entities in "key sectors" are prohibited from procuring network products and services that have not passed the security review. Other operators of CII can potentially procure unreviewed network products and services if such procurement would not affect national security.

The draft Measures leave two important questions open: First, it is unclear whether any sectors other than finance, telecommunications, and energy will be deemed "key sectors" under Article 10. It is also unclear whether Article 10 corresponds to any particular provisions in the Cybersecurity Law. Second, the draft Measures do not explain criteria for determining whether procurement will have an effect on China's national security. CAC, the agency tasked with protecting China's CII, is charged with setting these criteria later.

Substantive Criteria: Secure and Controllable

In conducting the review, the agencies will focus on whether the products and services are "secure and controllable." More specifically, the agencies will assess the following risks:

- The risk of products or services being unlawfully controlled, interfered with, or interrupted;
- The risks associated with research and development, delivery, and technical support of products or key parts;
- The risks associated with products or services being used by their suppliers to illegally collect, store, process, or utilize users' data;
- The risk of product or service providers using customers' reliance on those products or services to engage in unfair competitive practices or otherwise harm consumers; and
- Other possible harms to national security and the public interest.

The term "secure and controllable" was initially introduced in the Guidelines on Promoting the Application of Secure and Controllable Information Technology Products (Circular 317) ("the Guidelines") by the China Banking Regulatory Commission's ("CBRC") in 2013. According to the Guidelines, "secure and controllable" products and technologies in the banking sector are those that are "capable of meeting the information security needs of the banking industry and whose *technical risks, outsourcing risks and supply chain risks* are controllable (emphasis added)." The Guidelines also mandated that "secure and controllable" products and technologies make use of domestic intellectual property rights. The Guidelines were later suspended amidst criticism from international stakeholders.

Although using the same expression, the draft Measures focus on different aspects of "secure and controllable," including, for example, whether the products or services may change their stated functions without the knowledge of users, whether users can retain control of their own data, or whether users are overly dependent on the products or services.

Review Agencies

Pursuant to the draft Measures, a Cybersecurity Review Commission ("the Commission") will be established, with CAC taking the lead in coordinating with other relevant ministries and agencies. The Commission will be responsible for shaping policies regarding the review and addressing key cybersecurity issues. Under the Commission, a Cybersecurity Review Office ("the Office") will be established to handle the actual review work.

In assisting the Office's review, two more groups will be involved in the process:

- Designated third party evaluation centers, whose technical evaluation reports will be used as the basis for evaluating the cybersecurity risks of products and services; and
- An expert panel assembled by the Commission, which will conduct comprehensive assessments of security risks associated with the products or services and evaluate whether the suppliers are "secure and controllable," on the basis of third party reports.

The Office will form its review decision based on the third party reports and the expert panel's recommendations.

Review Process

The draft Measures provide that the Office can initiate security reviews in response to requests made by government agencies, suggestions made by trade associations, or incidents in the market. Companies can voluntarily submit their products or services for review as well (Article 8)

The review will typically consist of four elements: lab testing, on-site inspection, online monitoring, and review of background information (Article 3). No further detail was provided with respect to how these elements will be carried out.

The draft Measures do not establish time limits for elements of the review or the overall timeframe for the entire review.

Conclusion

The release of the draft Measures for public comment is a step forward in the government's effort to formalize the procedures for cybersecurity reviews mandated by the Cybersecurity Law. However, given the present lack of clarity regarding substantive criteria and procedures that will

be applied during the review process, suppliers of network products and services will need to proceed cautiously. In managing these uncertainties, companies should assess carefully the pros and cons of voluntarily submitting their products or services for review, and also evaluating the possible risk that interested third parties may seek to encourage such a review.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com