COVINGTON

China Releases Final Regulation on Cybersecurity Review of Network Products and Services

May 3, 2017

Data Privacy and Cybersecurity

On May 2, 2017, the Cyberspace Administration of China ("CAC") released the final version of the *Measures on the Security Review of Network Products and Services (Trial)* ("the Measures"), with an effective date of June 1, 2017 (official Chinese version available here; Covington's translation of the Measures is appended at the end of this alert. Amendments to draft Measures in redline). The issuance of the Measures marks a critical first step toward implementing China's Cybersecurity Law ("the Law"), which was promulgated on November 7, 2016 and will take effect on June 1, 2017 (the same date as the Measures).

The long-anticipated Measures offer guidance on how CAC is planning to conduct cybersecurity reviews of network products and services procured by entities in a range of key sectors and other operators of Critical Information Infrastructure ("CII"), if the procurement "may affect China's national security."

A draft form of the Measures was released in February 2017 for public comment (see Covington's alert on the draft Measures here). Since then, international stakeholders have been submitting comments to the CAC, and changes in the final version reflect some of these comments. The Measures, however, still lack clarity with respect to certain aspects of the review process, both in terms of substantive criteria and procedure. Companies that may be subject to such reviews will likely need further guidance from the agencies once the Measures take effect.

Key changes in the final version of the Measures include:

- A potentially narrowed scope of products subject to cybersecurity review;
- Revised substantive criteria with an increased focus on supply chain risks;
- A revised review process; and
- New provisions introducing accountability.

Background

Article 35 of the Cybersecurity Law institutionalized 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 "cybersecurity review."

The Measures—the first implementing regulation of the Cybersecurity Law—aim to implement Article 35. After the February draft, the CAC considered comments from stakeholders and

updated the regulation. While some criteria have been updated, many other important points remain unclear, including the timing of the process and the concrete procedure for the review.

Potentially Narrowed Scope of Review

In the final version, only procurement of "important network products and services" related to network and information systems that implicate China's national security will be subject to the cybersecurity review (Article 2). Although the previous draft provided that network products and services that implicate "public welfare" would be subject to review, this "public welfare" standard has been removed in the final version. This change signals a potentially significant narrowing of the scope of the review so long as "national security" is not interpreted more expansively. And still, the term "important network products and services" remains undefined.

The final version clarifies that suppliers to two types of entities may be subject to the review process:

- Entities in key sectors, such as telecommunication and information services, energy, transportation, water conservation, finance, utilities and e-government; and
- Other operators of CII.

The final version, however, no longer creates a two-tiered system, but requires uniformly that for these entities, any procured network products and services that may affect China's national security have to pass the review (Article 10). Whether a procurement may affect China's national security will be determined by "the authority that is responsible for protecting [CII]," which is likely to be industry regulators in the key sectors identified above.

Revised Substantive Criteria with an Increased Emphasis on Supply Chain Risks

In the February draft, reviewing agencies were instructed to focus on whether the products and services are "secure and controllable." The final version expands this analysis to cover the supply chains of products and services as well (Article 3).

With this in mind, the risk criteria agencies will assess include:

1. Security risks inherent in the products or services themselves, as well as the risk that the products or services will be unlawfully controlled, interfered with, or interrupted;
2. Supply chain security risks associated with all stages of the life cycle (i.e., manufacturing, testing, delivery, and technical support) of products and key components;
3. The risks associated with products or services being used by their suppliers to illegally collect, store, process, or use users' data;
4. The risks that product or service providers could negatively impact cybersecurity or consumers' rights and interests by leveraging customers' reliance on the products or services. (The final version removes the reference to "unfair competitive practices"); and
5. Other risks that may compromise national security.

Government-designated third-party evaluation centers, whose technical evaluation reports will be used as the basis for evaluating the cybersecurity risks of products and services, are also required to evaluate whether the products and services, as well as their supply chains, are "secure", "controllable" and "transparent (in relation to the security mechanism and technologies)."

Revised Review Process

The final Measures provide that the Cybersecurity Review Office (the "Office") must identify review targets "in accordance with procedure." Although the February draft Measures contemplated that companies could voluntarily submit their products or services for review, this provision was removed in the final version. Instead, the Office can initiate cybersecurity reviews based on "relevant requirements" imposed by the government, suggestions made by national trade associations, or feedback by users.

The roles of two other groups—government-designated third-party evaluation centers and expert panels—remain unchanged in the final Measures. Expert panels, assembled by the Cybersecurity Review Commission ("the Commission"), will still 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.

The final version still contemplates that the review will 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 Measures still do not establish time limits for elements of the review or the overall timeframe for the entire review.

Provisions for Reporting Misconduct of Third-Party Evaluation Centers

Because third-party evaluation centers play an important role in the cybersecurity review process, the final version of the Measures includes new provisions designed to introduce accountability. Specifically, providers of network products and services can report third parties to the Office or to the "relevant departments" if those third parties fail to act objectively and fairly, or if they fail to maintain confidentiality over the information obtained during the review process.

Conclusion

Though the final version of these Measures adds some clarity to the February draft Measures, much uncertainty remains. Given the lack of clarity regarding substantive criteria and procedures that will be applied during the review process, suppliers of network products and services should proceed cautiously. Moreover, given the increased emphasis on the supply chain of these products and services, suppliers of network products and services should be mindful of security risks running through their entire supply chain.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
Jenny Martin	+1 650 632 4737	jrmartin@cov.com
Ted Karch	+1 415 591 7094	tkarch@cov.com

Covington Unofficial Translation

非官方翻译，科文顿·柏灵律师事务所敬上

Measures on the Security Review of ~~Online~~Network Products and Services

(~~Draft for Comments)~~For Trial Implementation)

Article 1 ~~The security and controllability of online products and services directly impact users' interests and relate to national security.~~ These Measures are established in accordance with the National Security Law of the People's Republic of China and the Cybersecurity Law of the People's Republic of China and other laws and regulations to enhance the controllable security level of ~~online~~network products and services, prevent ~~supply chain~~network security risks, and safeguard national security ~~and public interests~~.

Article 2 Important ~~online~~network products and services ~~used in the~~procured for network and information systems that relate to national security ~~and public interests~~ shall be subject to ~~the~~ cybersecurity review.

Article 3 The cybersecurity review shall be conducted for ~~online~~network products and services and their supply chains by the combination of businesses' commitments with social supervision, the combination of third parties' evaluation with the government's continuous regulation, and the combination of laboratory testing, on-site inspection, online monitoring and review of background information.

Article 4 The cybersecurity review shall be focused on the security and controllability of ~~online~~network products and services, including, among others:

(1) The ~~risk of~~security risks to the products or services themselves and risk of the products or services being unlawfully controlled, interfered with, or interrupted;

(2) The supply chain security risks associated with ~~research and development~~manufacturing, testing, delivery, and technical support of products or key ~~parts~~components;

(3) The risks associated with products or services being used by their suppliers to illegally collect, store, process, or ~~utilize~~use users' data by taking advantage of the favorable conditions created by the products and services;

(4) The risk of product or service providers using customers' reliance on those products or services to ~~engage in unfair competitive practices or otherwise~~ harm cybersecurity and consumers' rights and interests; and

(5) Other risks that may compromise national security ~~and public interests~~.

Article 5 The National Internet Information Office shall work with ~~related~~relevant departments to establish a Cybersecurity Review Commission which shall be responsible for reviewing important policies for cybersecurity review, organize the cybersecurity review tasks, and coordinate important issues related to the cybersecurity review.

The Cybersecurity Review Office shall be responsible for the implementation of the cybersecurity review.

Article 6 The Cybersecurity Review Commission shall engage related experts to establish an expert panel which shall, based on third-party evaluation, conduct a comprehensive evaluation of the security risks of ~~online~~network products and services and the security reliability of the providers of such products and services.

Article 7 Third-party cybersecurity review agencies shall be ~~exclusively~~ identified by the government in accordance with the law and shall perform third-party evaluation services in the cybersecurity review.

Article 8 Based on ~~the~~relevant government requirements ~~of related government departments~~, suggestions of national trade associations, ~~market~~user feedback ~~and corporate applications,~~ etc., the Cybersecurity Review Office shall identify review subjects in accordance with procedure and organize third-party agencies and ~~experts~~expert commissions to conduct cybersecurity review of ~~online~~network products and services and publish or circulate to a certain extent the review results.

Article 9 The competent government departments of key industries and sectors such as finance, telecommunications ~~and~~, energy and transportation shall organize the implementation of the cybersecurity review of ~~online~~network products and services in their respective industries or sectors pursuant to the requirements for the national cybersecurity review.

Article 10 ~~The Party and government departments as well as key industries shall give priority to online products and services that have passed the review in procurement, and shall not procure any online products or services that fail to pass the review.~~**~~Article 11~~** ~~Where any online products or services that are purchased by~~Where operators in important industries and sectors, such as telecommunication and information services, energy, transportation, water conservancy, finance, public services, e-government, and other operators of critical information infrastructure ~~operators~~procure network products or services that may affect national security, such products or services shall ~~be subject to the~~undergo a cybersecurity review. Whether ~~any~~ products or services affect national security shall be determined by the authority that is responsible for protecting critical information infrastructure.

Article 1~~2~~1 Third -party agencies performing the cybersecurity review shall adhere to the principles of objectivity, fairness and justness, according to relevant government requirements and with reference to relevant standards, and carry out evaluation ~~of online products and services and providers~~ focusing on the security and controllability of the products, services and supply chains, transparency ~~and creditability,~~of the security mechanism and be responsible for the review results.

Article ~~13~~12 Providers of ~~online~~network products and services shall cooperate in the cybersecurity review and be responsible for the authenticity of the materials provided.

Third -party agencies and related organizations and personnel shall undertake ~~the~~ security and confidentiality obligations for any information learned in the review, and shall not use such information for any purpose other than the cybersecurity review.

Article ~~14~~13 The Cybersecurity Review Office will issue the security evaluation reports for ~~providers of online~~network products and services from time to time.

Article 14 Providers of network products and services can report to the Cybersecurity Review Office or relevant departments when they consider that third party institutions and other relevant entities and individuals lose objectivity and fairness or fail to bear the confidentiality obligations relating to information obtained during the review process.

Article 15 ~~AnyThe National Internet Information Office shall be responsible for the interpretation of these Measures.~~Any violation of the provisions in these measures shall be dealt with in accordance with relevant laws and regulations.

Article 16 These Measures shall come into force as of ~~[DATE],~~June 1, 2017.