漢坤律師事務所
HAN KUN LAW OFFICES

Written by
David Tang and Min Zhu

The Unveiling of Cybersecurity Reviews

Contents:

On May 2, 2017, the Cyberspace Administration of China ("CAC") issued a trial version of the Measures for the Security Review of Network Products and Services (Trial) ("Trial Measures"), which are slated to become effective on June 1. The Trial Measures are another supporting document of the Cybersecurity Law that is intended to enact the cybersecurity review requirements of Article 35 of the Cybersecurity Law, following its issuance on November 7, 2016.

1. Changes in the Trial Measures

Compared to the original draft for comment version of the measures ("Draft") issued by CAC on February 4, 2017, the Trial Measures make a number of clear adjustments, which mainly include:

a. References to the "public interest" have been removed throughout the regulation. We understand that "public interest" is an ambiguous and broad concept that may lead to a scope that is beyond the boundaries of the cybersecurity review. Thus, the removal of public interest provides for a clearer regulatory scope for the Trial Measures, and is also more in line with the original focus of national cyber-security review.

b. The security review criteria have been made clearer. The Trial Measures expressly stipulate that the cybersecurity review includes static reviews (security risks of the products and services themselves) and dynamic reviews (supply chain security risks to products and key components, including in the process of production, testing, delivery and technical support), based on the secure and controllable requirements.

c. Reiteration of key industries and sectors. In coordinating with the Critical Information Infrastructure ("CII") provisions in Article 31 of the Cybersecurity Law, the Trial Measures reiterate that the key areas subject to cybersecurity reviews are public communications, information services, energy, transportation, water conservancy, finance, public services and e-government, and others key industries and sectors. It is worth mentioning that the Trial Measures remove the "party and government offices" language found in the Draft. We understand that party and government offices have their own security review mechanism, so it is unnecessary to specifically regulate these entities in the Trial Measures.

2. Main Content of the Trial Measures

The Trial Measures contain the following aspects that are worthy of note:

a. No administrative access approvals, focus on concurrent and post-event regulation

Throughout the Trial Measures, emphasis is placed on concurrent and post-event regulation rather than setting new market access administrative licensing for network product and service providers.

The Trial Measures stipulate in Article 2 that "important network products and services purchased for networks and information systems that relate to national security must pass a cybersecurity review."

Article 3 further provides that "cybersecurity reviews of network products and their providers and supply chains shall be carried out by a combination of enterprise commitment and social supervision,

of third-party evaluations and continuous government oversight, and of laboratory testing, on-site inspections, online monitoring and background investigations."

b. Security Review Criteria: Secure and controllable

From the outset of cybersecurity legislation, "secure" and "controllable" have been the two concepts that are most referred to by legislators and regulators, and the Trial Measures again confirm these concepts as the basic principles guiding the Cybersecurity Law and its implementation. Article 4 of the Trial Measures states that security reviews shall focus on security and controllability, including: 1) security risks of the products and services themselves, and the risk of being illegally controlled, interfered with or interrupted in the course of operating; 2) supply chain security risks to products and key components; 3) risk of illegal collection, storage, processing and use of user information by providers of such products and services; 4) risks of harming cybersecurity and users' interests, and 5) other risks that may harm national security.

Of these criteria, 1) and 2) evaluate the ability to defend against risks, and 3) and 4) prohibit active infringing conduct. These criteria give consideration to both the active and passive aspects of cybersecurity, but remain concepts in principle. Without further guidance, it is difficult to predict the scope and standard of cybersecurity reviews in practice, and the relevant reviewers appear to be left with broad discretion in this regard.

c. Multi-party participation, striving for due process

The Trial Measures primarily place emphasis on the cybersecurity review process, as shown by Articles 5 to 10. These articles reflect administrative participation and due process under the modern administrative procedure law.

For example, from the perspective of participants, the Trial Measures involve the cybersecurity review commission (a newly established agency), cybersecurity review office, cybersecurity review experts committee, third-party institutions, national industry associations, users, competent departments in their respective industries and sectors, CII protection departments, and, from the perspective of process, the Trial Measures refer to expert evaluations, social supervision and public participation, among others.

It is clearly observable, however, that the final decisions relating to cybersecurity reviews are to be made by government regulators. Therefore, in contrast to the principle of simplifying administrative procedures, referred to as "small government and big society," legislators still desire to exert a certain degree of greater governmental power in the area of cybersecurity.

d. Reviews to be commenced by regulatory departments

The Trial Measures also make clear the procedures for launching cybersecurity reviews. Article 8 of the Trial Measures state that the cybersecurity review office shall commence security reviews in accordance with the relevant national requirements, and take into consideration the suggestions of national industry associations and user feedback. Article 9 requires that competent departments of key industries and sectors, such as finance, telecommunications, energy and others, shall organize cyber-security reviews of network products and services within their respective industries and sectors ac-cording to the national cybersecurity review requirements.

Compared to the Draft, the Trial Measures remove the application by enterprises as an option to commence cybersecurity reviews. That is to say, enterprises no longer have the right to initiate security reviews, and, in necessary situations, most can only promote security reviews via industry associations or other indirect means. This is also consistent with the government's position mentioned above, the government is inclined to adopt active administration and proactive regulation for cybersecurity matters.

Stefano Beghi
Tel. + 852 21563490
sbeghi@gop.it

Davide De Rosa
Tel. + 852 21563490
dderosa@gop.it

e. Security assessment reports: A black list for cybersecurity reviews?

Article 13 of the Trial Measures state that the cybersecurity review office will release assessment reports on the security of network products and services from time to time. No report format or content requirements have currently been provided. However, information we have gathered from the legislative process suggests that the assessment reports will not only include information on network pro ducts and services and their providers that pass reviews, but will also include a listing of those pro-ducts, services and providers that have not passed. This information may be developed into an information disclosure system based on the "white list" and "black list," that may affect and direct the industry guidance.

In addition, a CAC official has said that the regulator will treat enterprises and products from China and other countries equally during cybersecurity reviews, and will not direct efforts at products and services from specific countries or regions, nor limit foreign products from entering the domestic market. However, as the cybersecurity reviews focus on "national security," it remains to be seen whether the reviews will raise certain invisible barriers to market access in China for products and services provided by foreign enterprises or domestic joint-ventures.

3. Advice

Strictly speaking, cybersecurity reviews for network products and services do currently exist. There are certain national quality standards, industries access and enterprise qualification requirements for special industries, products and services, and enterprises themselves may have their own product security and industry standards. Until now, however, no specialized regulation has been enacted to confirm a unified system and standard for such cybersecurity reviews. The issuance of the Trial Measure marks the commencement of nationally-led cybersecurity reviews.

The Trial Measures are still a basic guidance for the cybersecurity review of network products and services based on its current content, which will require further development and refining. Such issues include, for example, organizing the cybersecurity review commission and experts committee, identifying third-party institutions, evaluating criteria that affect national security and related review processes and working rules.

While detailed regulations are on the way, the related penalties are clear. According to Article 65 of the Cybersecurity Law, CII operators using products or services which have not undergone or have failed security reviews will be ordered by the competent department to stop such use and may be subject to a fine equivalent to more than 1 but less than 10 times the purchase price, and the supervisor directly in charge and other persons directly responsible will be subject to fines ranging from 10,000.00 yuan to 100,000.00 yuan. It can thus be said that the penalty ceiling is relatively high.

We would therefore recommend that network operators and providers of network products and services, especially CII operators in key industries and sectors, conduct self-reviews of network products and services they have purchased or which they provide to others in order to make improvements according to the secure and controllable requirement, and keep open communications with industry regulators and industry associations, and to watch for further developments in this area.

Gianni, Origoni, Grippo, Cappelli & Partners and Han Kun Law Offices have an alliance agreement. Both firms have a wide range experience in Cybersecurity: for any advice or assistance, contact us!