Legal Commentary

May 6, 2020

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Legal Commentary on the Measures for Cybersecurity Review

Authors: David TANG | Effy SUN[1]

On April 27, the Cyberspace Administration of China ("**CAC**") and 11 other departments[2] jointly announced the promulgation of the *Measures for Cybersecurity Review*[3] (the "**Measures**"), which will come into effect on June 1, 2020 and replace the current *Measures for Security Review of Network Products and Services (for Trial Implementation)*[4] (the "**Trial Measures**"). The Measures aim to ensure the security of supply chains for critical information infrastructure ("**CII**") and guarantee national security by prescribing a security review by the Cybersecurity Review Office (the "**CRO**") for certain network products and services purchased by CII operators.

Background

The Measures were formulated on the basis of the *National Security Law of the People's Republic of China*[5] and the *Cybersecurity Law of the People's Republic of China*[6] (the "**Cybersecurity Law**").

---

[1] Special thanks to John Fitzpatrick for his contributions to the writing of this article.

[2] The 12 departments jointly announcing the Measures are: the Cyberspace Administration of China, the National Development and Reform Commission of the People's Republic of China, the Ministry of Industry and Information Technology of the People's Republic of China, the Ministry of Public Security of the People's Republic of China, and the Ministry of National Security of the People's Republic of China, the Ministry of Finance of the People's Republic of China, the Ministry of Commerce of the People's Republic of China, the People's Bank of China, the State Administration of Market Supervision and Administration, the State Administration of Radio and Television, the State Secrets Administration, and the State Encryption Administration.

[3] 《网络安全审查办法》[Measures for Cybersecurity Review] (Cyberspace Admin. China et al., Decree No. 6; promulgated Apr. 13, 2020, effective June 1, 2020) [hereinafter "**Measures**"], available at http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.

[4] 《网络产品和服务安全审查办法（试行）》[Measures for Security Review of Network Products and Services (for Trial Implementation)] (Cyberspace Admin. China; promulgated May 2, 2017, effective June 1, 2017), available at http://www.cac.gov.cn/2017-05/02/c_1120904567.htm.

[5] 《中华人民共和国国家安全法》[National Security Law of the People's Republic of China] (Standing Comm., Nat'l People's Cong., Pres. Order No. 29; promulgated and effective July 1, 2015) 2015 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 4 at 701.

[6] 《中华人民共和国网络安全法》[Cybersecurity Law of the People's Republic of China] (Standing Comm. Nat'l People's Cong., Pres. Order No. 53; promulgated Nov. 7, 2016, effective June 1, 2017) 2016 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 6 at 899.

In relevant part, the Cybersecurity Law requires CII operators to pass a security review where their procurement of network products or services affect or may affect national security[7]. This requirement was initially implemented in 2017 through promulgation of the Trial Measures.

The Trial Measures present the basic framework for cybersecurity reviews, which is retained in the Measures[8]. The Trial Measures emphasize reviewing the products and services based on their effect on national security notably through the lenses of "security" and "controllability," two factors which have concerned the foreign business community due to their openness to interpretation and their potential to constitute technical barriers to trade[9]. CAC issued a consultation draft of the Measures in May 2019[10] (the "**Consultation Draft**") which, for purposes of cybersecurity reviews, emphasized national security and proposed to further refine the concept of "secure and controllable"[11] for the products and services.

Possibly in response to such concerns, the Measures no longer use "secure and controllable" as a principle for review, while some of its underlying policy objectives are instead relegated to contractual undertakings between CII operators and providers of products or services[12]. Compared with the Consultation Draft, we believe the Measures clarify the cybersecurity review process in three significant ways: (a) further easing the review criteria, focusing on protection of national security, CII security, and violations of Chinese law, (b) monitoring CII operation security and stability when using relevant products and services, and (c) specifically identifying certain types of network products and services that are subject to review.

Highlights of the Measures for Cybersecurity Review

I Competent regulatory authorities

The Measures stipulate that the 12 drafting authorities will establish a national cybersecurity review mechanism under the leadership of the Central Cyberspace Affairs Commission[13]. The CRO is responsible for formulating the relevant system specifications for and organizing cybersecurity reviews[14]. Certain regulatory authorities considered "mechanism member units and relevant CII protection departments" are responsible for second-level reviews after the preliminary review by the

[7] *Id.* at Art. 35.

[8] A separate review process has been implemented for cloud computing services providers which serve CII operators and Party organizations. 《云计算服务安全评估办法》[Measures for Security Assessment of Cloud Computing Services] (Cyberspace Admin. China et al., Ann. [2019] No. 2; promulgated July 2, 2019 effective Sept. 1, 2019), available at http://www.cac.gov.cn/2019-07/22/c_1124781475.htm.

[9] E.g., *Statement by the European Union on the Committee on Technical Barriers to Trade on March 6 and 7 2019*, Council for Trade in Services G/TBT/W/637, Doc. #19-2261, Apr. 9, 2019 ("Concepts such as … 'secure and trustworthy products' are not sufficiently clarified.").

[10] 《网络安全审查办法（征求意见稿）》[Measures for Cybersecurity Review (Draft for Comment)] (Cyberspace Admin. China; issued on May 21, 2019 for public comment until June 24, 2019), available at http://www.cac.gov.cn/2019-05/24/c_1124532846.htm.

[11] "Secure and controllable means that product and service providers must not use the convenience of providing products and services to illegally obtain user data, illegally control and manipulate user equipment, or use the user's dependence on the products and services to obtain illegitimate benefits or force users to update and replace, etc." Measures for Cybersecurity Review (Draft for Comment), Art. 18.

[12] Measures, Art. 6.

[13] Measures, Art. 4.

[14] Measures, Art. 4.

CRO[15]. CII protection departments may formulate cybersecurity review prejudgment guidance and identify CII operators in their respective sectors, and will conduct second-level reviews in conjunction with the mechanism member units[16].

II Initiating cybersecurity reviews – two methods

1. CII operator-initiated reviews

Generally, CII operators which plan to procure network products or services should evaluate the national security risks that the products or services may pose before placing the products or services into use and, if risks are believed to exist, apply for a review to the CRO. The CRO will then determine whether the products or services require review.

2. Regulatory authority-initiated reviews

Where any member unit of the cybersecurity review mechanism believes that a network product or service affects or may affect national security, the CRO can submit an application to the Central Cyberspace Affairs Commission to obtain approval for a cybersecurity review, and subsequently conduct a review in accordance with the procedures under the Measures[17].

III Review procedures

The CRO is to complete cybersecurity reviews within 30-45 days and submit the review results to mechanism members and relevant CII protection departments for a second review, which may take up to 15 days[18]. If the departments have different opinions on the review results, the CRO will initiate a special review and submit the results to the Central Cyberspace Affairs Commission for a final decision[19].

In addition, though the CRO is responsible for cybersecurity reviews, a CAC official has indicated that authorization will be granted to the China Cybersecurity Review Technology and Certification Center to conduct specific work, including receiving application materials, form reviews of application materials, and organizing review work[20].

IV Clarity for cybersecurity reviews

1. Scope of CII operators

The stated purpose of the cybersecurity review mechanism is to protect the security of CII and national security. However, the scope of CII remains uncertain due to underdevelopment of the relevant regulations. CAC has stated in relation to the cybersecurity review process that network operators

[15] Measures, Art. 11.

[16] Measures, Art. 5.

[17] Measures, Art. 15.

[18] Measures, Arts. 10, 11.

[19] Measures, Art. 12.

[20] 《网络安全审查办法》答记者问 [News Briefing on the Measures for Cybersecurity Review] (Cyberspace Admin. China, Apr. 27, 2020) at Question 10, available at http://www.cac.gov.cn/2020-04/27/c_1589535446378477.htm.

may be required to apply for cybersecurity reviews where they operate in any of the following industries: telecommunications, broadcasting, energy, finance, road and waterway transportation, railway, civil aviation, postal service, hydraulic engineering, emergency management, healthcare, social security, and national defense technology[21]. It appears that the scope of CII cited by the official is broader than the seven industries specified in the Cybersecurity Law and we expect that the scope of CII will be clarified in further legislation. Before that time, it is still advisable to consult with the competent authorities to determine whether your business is classified as a CII so as to comply with the requirements of the Measures.

2. Scope of products and services

The Measures provide clarity as to what types of products or services are important and require review before use by CII operators. The types include core network equipment, high-performance computers and servers, mass storage devices, large databases and application software, network security equipment, cloud computing services, and other products and services that have an important impact on the security of CIIs[22]. Note that a cybersecurity review process is only required after the CII operator preliminarily determines that a proposed procurement of the specified products or services may expose the CII to national security risks.

3. Review criteria

The review criteria in the Measures concentrate on the impact of the products and services on the stability, security and continuity of the CII. To illustrate the change and development of review criteria, we have prepared a comparison of review criteria of the Trial Measures, the Consultation Draft, and the Measures as below:

Cybersecurity Review Criteria

Trial Measures (Art. 4)	Consultation Draft (Art. 10)	Measures (Art. 9)
Cybersecurity reviews focus on reviewing the security and controllability of network products and services, which mainly includes:	Cybersecurity reviews focus on the assessment of possible national security risks from procurement activities, which mainly consider the following factors:	Cybersecurity reviews focus on assessing the possible national security risks of procuring network products and services, which mainly consider the following factors:
■ The security risks of products and services, as well as the risks of illegal control, interference and interruption of operations;	■ The impact on the continuous safe and stable operation of CII, including the possibility that the CII is controlled, interfered with, and business continuity is compromised;	■ The risk to the CII brought by the use of products and services being illegally controlled, subject to interference or destruction, and the theft, leakage, or damage of important data;
■ The risk of product and	■ The possibility of causing a	

[21] News Briefing on the Measures for Cybersecurity Review, Question 4.

[22] Measures, Art. 20.

Trial Measures (Art. 4)	Consultation Draft (Art. 10)	Measures (Art. 9)
service providers illegally collecting, storing, processing, and using user-related information using the convenience of providing products and services;	large amount of personal information and important data to be leaked, lost, damaged, and transferred cross-border;	
■ Supply chain security risks during production, testing, delivery, and technical support of products and key components;	■ Controllability, transparency and supply chain security of products and services, including the possibility of interruption of product and service supply due to non-technical factors such as political, diplomatic, and trade;	■ The disruption of the supply of products and services to the business continuity of CII;
		■ The security, openness, transparency, diversity of sources, reliability of supply channels, and the risk of supply disruption due to political, diplomatic, and trade factors;
/	■ The impact on defense-related military industry, CII-related technologies and industries;	/
/	■ Product and service providers' compliance with national laws and administrative regulations, as well as their commitments and responsibilities;	■ Product and service providers' compliance with Chinese laws, administrative regulations, and departmental regulations;
/	■ Circumstances where the products and service providers are funded and controlled by foreign governments;	/
■ The risk that product and service providers use users' dependence on products and services to damage cybersecurity and user interests;	■ Other factors that may jeopardize the security of CII and national security.	■ Other factors that may jeopardize the security of CII and national security.
■ Other risks that may endanger national security.		

As stated earlier, the Measures emphasize protection of national security and refine the concept of "secure and controllable," aiming to achieve its policy objectives through contractual undertakings between the providers and CII operators, rather than regulators scrutinizing compliance with the criteria. The undertakings include cooperating in the cybersecurity review process, which includes not taking advantage of the provision of services to illegally collect users' personal information, control or manipulate users' equipment, or interrupt the supply of products or necessary technical support services without justifiable reasons, etc.[23] From this perspective, it appears that CII operators will now have more freedom in choosing providers of network products or services, although it remains unclear to what extent CII operators may practically involve a provider of products or services in the review process to ensure its procurement is in compliance with the Measures.

The Measures also delete several non-technical enumerations such as (a) the impact on China's national defense and military industries and CII-related technologies and industries, and (b) circumstances where providers of products or services are funded or controlled by foreign governments. Notwithstanding the deletions which we believe are to ensure the technicality and neutrality of cybersecurity reviews, most of the criteria in the Measures remain substantively unchanged as compared with the Consultation Draft, e.g. the risk of supply disruption due to "political, diplomatic, and trade" factors and a catch-all clause. Moreover, the criteria enumerated are general principles without detailed guidance, so it remains practically uncertain for parties involved in CII procurement to have a clear path to comply with the Measures. We expect that the industry regulators and the CRO will work together to issue detailed standards or guidance to improve the certainty of the review process.

V Contracts for network products or services advised to be conditioned upon review

The Consultation Draft proposed conditioning the effectiveness of procurement contracts between providers of products or services and CII operators upon passage of a cybersecurity review[24]. While the Measures do not have this requirement, as CAC advises, we would recommend that the parties to such contracts first pass the cybersecurity review process or condition contract performance on passing the review[25].

Our Observations

The promulgation of the Measures follows a number of other recent proposed and effective departmental rules which appear to relax regulatory oversight and adopt a contract-oriented approach compared to earlier proposed rules, including the 2019 *Measures for Security Assessment of Cross-border Transfer of Personal Information (Draft for Comment)*[26], and provide greater clarity for CII operators in making procurement decisions, potentially helping to level the playing field for foreign providers of network

[23] Measures, Art. 6.

[24] Measures for Cybersecurity Review (Draft for Comment), Art. 7.

[25] News Briefing on the Measures for Cybersecurity Review, Question 5.

[26] 《个人信息出境安全评估办法（征求意见稿）》[Measures for Security Assessment of Cross-border Transfer of Personal Information (Draft for Comment)] (Cyberspace Admin. China; issued for public comment on June 13, 2019 until July 13, 2019), available at http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

products and services. Compared to the Trial Measures, in anticipation of more details on review guidance and standards from the CRO, we believe the Measures reflect a more tempered approach to the cybersecurity review process — balancing concerns over national security and technical barriers to trade. That said, given the ambiguities in certain review criteria, it is unsurprising that CII operators, in particular core Chinese industrial CII operators, may, similar to practices in other countries, retain the initiative in selecting domestic providers over foreign providers of products and services, and cybersecurity reviews may cause foreign providers to be less competitive in procurement decisions. We will continue monitoring the practical and legal developments in this regard.

In light of the Measures, CII operators will need to conduct a self-examination to identify whether there is any product or service in use or to be used which falls within the scope of review. If yes, the CII operator may need to submit a review application to the CAC and arrange for the procurement agreement to be subject to the review result. As mentioned earlier, the CII operator must also ensure that all the obligations of review assistance including various security commitments are imposed in the procurement agreements. It may also be advisable to improve internal procurement processes to fully account for cybersecurity reviews.

If you are a provider of products or services, regardless of whether you are a foreign or domestic entity, even though you are not responsible for cybersecurity review applications, it is still suggested that you confirm with your customers their CII status. If they operate CII, you may need to prove to your customers that your products or services do not fall within the scope of the review criteria or that you can fulfill the contractual obligations to ensure relevant CII operation security. It is likely that you will have to customize materials for different CII customers when demonstrating capabilities and assisting in the review process. You may even wish to consider a local entity to logistically facilitate the process. Further, confidentiality commitments must be included in the procurement agreements to ensure the customers' non-disclosure obligations during the review process.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

David TANG

Tel: +86 21 6080 0905
Email: david.tang@hankunlaw.com