WAPACK LABS
CYBER INTELLIGENCE SERVICE

TLP GREEN

INTELLIGENCE REPORT

SERIAL: IR-19-151-001
COUNTRY: CN
REPORT DATE: 20190531

CHINA MODIFIES CYBERSECURITY LAW IN POSSIBLE RETALIATION FOR HUAWEI BAN

SUMMARY

The Cyberspace Administration of China (CAC) issued a new draft cybersecurity regulation on 21 May 2019. This draft is a planned extension of the Cybersecurity Law issued in 2017 that placed greater restrictions on foreign firms operating in China. The new regulation creates the requirement for review of imported network equipment to determine if such equipment represents a risk to national security. The vagueness of the language indicates that the new law could be used to block the import of almost any US - manufactured network hardware.

Figure 1. Logo at CAC website

The language of this draft sets up the requirement for review if, "operators [are] procuring network products and services that could influence national security." Some provisions indicate this would include any equipment that might face, "supply chain security threats." This presumably means that equipment which could be manufactured with corrupt components, or were technically compromised enroute, would be potential national security risks. The draft additionally calls for review if, "the supply chain security of a product or service could be disrupted due to non-technical factors like politics, diplomacy, and trade." The draft also includes catch-all language that would trigger a review if, "other risks and dangers" were suspected. Any suspicious imports are to be reported to the CAC Cybersecurity Review Office, and all cases will be submitted from the CAC up its chain to the Central Cybersecurity and Informatization Commission for approval.

The draft was issued one week after the US executive order that blocked US companies from doing business with Huawei for national security reasons. The timing suggests that this regulation is being put into place as a counter to US actions, setting the conditions for blocking US equipment imports into China in retaliation for the moves against Huawei.

BACKGROUND: CYBERSECURITY LAW 2017

On 7 Nov 2016, the China National People's Congress passed a new and comprehensive Cybersecurity Law that went into effect on 1 Jun 2017. The CAC played a major role in formulating the Cybersecurity Law and is responsible for enforcing it.

The stated goals of the 2017 Chinese Cybersecurity Law were protection of personal information and standardization of collection and use practices for personal information. Key elements of the Law as published, have implications for foreign businesses, including the following:

- Businesses are obliged to employ network security safeguards such as contingency plans for handling network security incidents, reporting security risks, and assisting Chinese authorities in investigating cybercrimes.

- Cyber security-related products and services have to be certified in advance by the Chinese government and meet safety inspection requirements before they can be marketed in China.

- Companies that collect or process personal data of Chinese citizens are supposed to keep that data within the territory of China. To transfer the data outside the country, they need to undergo a security assessment and get approval from the Chinese government.

The Cybersecurity Law applies to all businesses in China, not just foreign enterprises, and there are provisions aimed specifically at government control over Internet content. However, some provisions such as restriction on cross-border data flow, may have greater impact on foreign entities accustomed to free data flow and storage outside China.[1]

In the two years following the Law's implementation by the CAC, a series of new regulations and guidelines were published in China that further constrained business operations and increased spending on cybersecurity practices. Some of the key provisions of the new measures include:

- The categories regulated now include cloud computing, big data, artificial intelligence, Internet of Things, and project control systems.

- Companies must provide the government all information on received cyberattacks and any "cyberthreat intelligence" in their possession.

[1] See Wapack Labs IR: U.S. Corporate Concerns with China's New Cybersecurity Law, 14 Jun 2017.

- Network operators must conduct self-reviews of their cybersecurity systems once a year and report risks and remediation plans to the Ministry of Public Security.

- Foreign businesses can now use only the virtual private networks (VPN's) that have been approved by the government.

On the surface, it appears the Law is designed to strengthen data protection and the security of critical information infrastructure. However, many of the provisions appear to actually be designed to facilitate the Chinese government's access to data held by domestic and foreign enterprises. There is also the suspicion that these measures are actually designed to make it harder for foreign companies to do business in China, making it easier for Chinese firms to compete.[2]

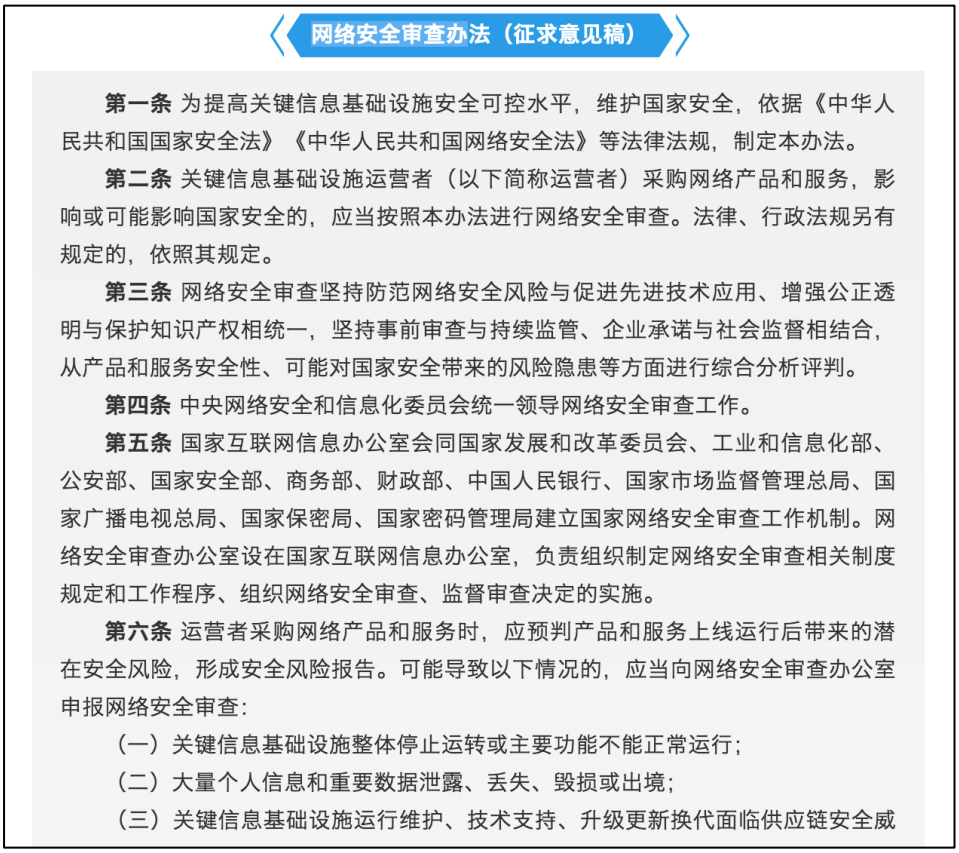
Cybersecurity Review Measures 2019

The draft "Cybersecurity Review Measures" was published for comment, a standard Chinese procedure that provides foreshadowing of planned law. **It is not clear from the enacting of previous cybersecurity measures that comments are actually accepted and incorporated into a draft. The comment period for these measures will close on 24 June 2019. This draft was identified and translated by Samm Sacks, Paul Triolo, et al, at New America, a Washington-based policy think tank that focuses on cybersecurity and international relations.[3]

As New America noted in the analysis that accompanied their translation, this draft law is one of a series of updates of the 2017 Cybersecurity Law that have been issued over the last two years, each providing greater detail on how the basic law will function. However, they also point out that the timing of the new release naturally ties this draft and its provisions to the US Executive Order and Commerce Department actions that effectively ban Huawei from business in the United States.[4]

The draft law does in fact provide a legal framework for claiming national security risks associated with technology imported into China, making it appear to be a mirror to the US actions that result in the Huawei ban.

[2] See Wapack Labs IR: One Year Under China's Cybersecurity Law, 16 Aug 2018.
[3] www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation.
[4] www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation.



网络安全审查办法（征求意见稿）

第一条 为提高关键信息基础设施安全可控水平，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条 关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。法律、行政法规另有规定的，依照其规定。

第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用、增强公正透明与保护知识产权相统一，坚持事前审查与持续监管、企业承诺与社会监督相结合，从产品和服务安全性、可能对国家安全带来的风险隐患等方面进行综合分析评判。

第四条 中央网络安全和信息化委员会统一领导网络安全审查工作。

第五条 国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部、国家安全部、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局建立国家网络安全审查工作机制。网络安全审查办公室设在国家互联网信息办公室，负责组织制定网络安全审查相关制度规定和工作程序、组织网络安全审查、监督审查决定的实施。

第六条 运营者采购网络产品和服务时，应预判产品和服务上线运行后带来的潜在安全风险，形成安全风险报告。可能导致以下情况的，应当向网络安全审查办公室申报网络安全审查：

（一）关键信息基础设施整体停止运转或主要功能不能正常运行；

（二）大量个人信息和重要数据泄露、丢失、毁损或出境；

（三）关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威

Figure 2. "Cybersecurity Review Measures (For Comment)" as found online at TenCent.com

Selected provisions of the new regulation are shown below, with Wapack Labs comments added where the provisions have potential impact on the export of U.S.-manufactured network equipment to China.

Cybersecurity Review Measures (Draft for Comment)[5]
Cyberspace Administration of China
May 21, 2019

Article 1: In order to improve the level of security and controllability of critical information infrastructure and protect national security, … these measures are formulated.

Article 2: Critical information infrastructure operators (hereafter referred to as operators) **procuring network products and services that influence or could influence national security** should conduct a cybersecurity review according to these measures.

[5] The Chinese version is available at: mp.weixin.qq.com/s/J8KGlWR8Wvea1m8feoF7rA.

COMMENT: This article explicitly requires a security review for any purchases that could impact national security, without stating any further guidelines for determining how such a judgment would be made. This strengthens the impression that the government gets to make a "black box" review without having to explain its decision. The term "critical information infrastructure" was defined in the 2017 Law so broadly that it includes "public communications and information services, energy, finance, transportation, water conservation, public services, e-governance," and other enterprises that could harm national security or the economy if damaged.

Article 5: The Cyberspace Administration of China … establishes a cybersecurity review work mechanism. **The Cybersecurity Review Office resides in the Cyberspace Administration of China.**

COMMENT: This clarifies that the CAC owns the review process. Other reporting has suggested that there is some conflict between the CAC and the Ministry of Public Security over who has ultimate authority for cybersecurity reviews. This draft states CAC's claim on that function.

Article 6: **When operators purchase network products and services**, the potential security risks of operating products and services once in operation should be anticipated, and a security risk report should be generated. **Where the following circumstances may occur, a cybersecurity review should be reported to the Cybersecurity Review Office:**

- A large volume of personal information and important data has been leaked, lost, damaged, or removed from the country;
- Critical information infrastructure equipment operations protection, technical support, and upgrades and replacement **face supply chain security threats**;
- **Other risks and dangers** seriously endangering critical information infrastructure equipment security.

COMMENT: The reference to, "supply chain security threats" here could be used to trigger reporting to the Cybersecurity Review Office any time that network equipment is purchased from abroad. The inclusion of, "other risks and dangers" makes the criteria for triggering a review broad enough to include almost any purchase.

Article 10: The cybersecurity review focuses on assessing the potential **national security risks brought about by procurement activities**, mainly considering the following factors:

- The possibility that large amounts of personal information and important data could be leaked, damaged, lost, or removed from the country, etc.;
- **The possibility that the controllability, transparency, and supply chain security of a product or service could be disrupted, including the possibility of disruption due to non-technical factors like politics, diplomacy, and trade**;
- Situations in which product or service providers are funded, controlled, etc., by foreign governments.

COMMENT: This article implies that a decision to block a purchase of foreign equipment could be made just on the possibility that the supply chain could be disrupted by political conflict. This provision seems motivated by Chinese unhappiness with the ongoing trade war in general and with the Huawei ban in particular, since it is Huawei's supply chain that is cut off by the US Executive Order. In any event, it makes clear that even the possibility of politics interfering with the supply chain could be enough justification to block the import of equipment.

Article 19: Where cybersecurity inspection work mechanism member work units believe **network product and service purchasing activities**, or information technology service activities influence or **may influence national security**, the Cybersecurity Review Office shall, according to procedure, report the matter to the Central Cybersecurity and Informatization Commission **for approval, and conduct inspections according to these Measures.**[6]

COMMENT: The Central Cybersecurity and Informatization Commission is the echelon in the government above CAC. Thus, the chain of events for approval (or that could block approval) starts with some inspection work unit raising the issue of national security to the CAC Review Office. Then, the CAC Review Office makes the issue known to its superior Commission, the CAC Review Office conducts inspections and presumably reports to the Commission, and the Commission makes its

[6] www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation.

decision. This suggests that it will be relatively simple to make an issue out of some planned imports but complicated to get approval.

ADDITIONAL COMMENTS

Composing the text of this for-comment draft was probably a lengthy procedure. It was published about a week after the 15 May 2019 issuance of the US "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." It is not clear that the Chinese draft was created in direct response to the executive order, was modified to add provisions that mirror the executive order, or perhaps it was drafted entirely ahead of action taken by the United States.

In any event, this draft provides a legal mechanism for responding to the US Commerce Department's Entities List, to which about 70 Huawei affiliates have now been added, with restrictions on the import of US high-tech products, if the equipment can be characterized as a risk to Chinese national security. The vague nature of the criteria given for such a characterization means that the import of equipment of almost any kind could be blocked by the use of this regulation.

No references have been found to the draft regulation in Chinese English-language media intended for international audiences. Issuing this draft with little fanfare suggests that the Chinese could be laying the groundwork for retaliation against the Huawei ban but they are not using it for leverage in ongoing trade negotiations. **If the Chinese had planned to talk about this action in trade negotiations, they would have published or described it in English media.

Contact the Wapack Labs for more information: 603-606-1246, or feedback@wapacklabs.com.

Prepared: Wapack Labs Asia Desk, Silkworm
Reviewed: B. Schenkelberg
Approved: J. McKee