Another step forward filling in blanks in the cyber security law or more questions than answers?

August 2017

Hogan Lovells

A Brief Analysis of the Draft Key Information Infrastructure Protection Measures

Overview and background

On 11 July 2017, the China Cyberspace Administration ("**CAC**") released the draft Key Security ("**Draft Regulations**") for public consultation, as another piece of key follow-on legislation to The People's Republic of China Cyber Security Law (see our briefings here) adopted on 6 November 2016 and effective from 1 June 2017 ("**Cyber Security Law**"). The consultation period of the Draft Regulations ends on 10 August 2017.

To date, the other follow-on legislation issued or pending pursuant to the Cyber Security Law includes:

- The Network Products and Services Security Review Measures (for Trial Implementation), issued on 2 May 2017, effective on 1 June 2017 ("**Security Review Measures**") [1]
- The Security Assessment of Cross-border Transfer of Personal Information and Important Data Measures, for which the second draft was issued on 19 May 2017 for public comment ("**Security Assessment Measures**") [2]
- Information Security Technology - Data Cross-Border Transfer Security Assessment Guidelines, issued on 27 May 2017 for public comment
- The Key Network Equipment and Cybersecurity-Specific Product Catalogue (Batch 1), issued on 6 June 2017 (the "**KII Equipment First Batch**") (together, the "**Supporting Legislation**").

Article 31 of the Cyber Security Law stipulates that the detailed scope of key/critical information infrastructure ("**KII**") and security protection measures for KII will be formulated by the State Council. Although the Draft Regulations were released in a CAC circular seeking public comment, the Draft Regulations appear to be the measures referred to in Article 31 of the Cyber Security Law:

- of all the provisions in the Cyber Security Law, the rules relating to KII have always attracted the most public attention, as KII operators are subject to the strictest obligations under the Cyber Security Law, especially with respect to data localization requirements and security review for purchases of network products and services. However, because the scope of KII was never made clear in the Cyber Security Law or Supporting Legislation, many multinational enterprises with a need to move data across borders or purchase overseas network products and services have been waiting with some trepidation for the release of the Draft Regulations, which were supposed to clarify the scope of KII. However, they will be disappointed once again if the Draft Regulations are finally promulgated in their current form, because the most highly anticipated answer is not provided – they only say that specific guidelines for identifying KII shall be formulated
- furthermore, under the Draft Regulations:
  - additional security obligations are imposed on KII operators
  - reporting obligations are imposed with respect to the remote operational maintenance of KII
  - additional security review requirements on systems or software developed by outsourcing, and on donated network products are imposed.

Refining the scope of KII

Article 18 of the Draft Regulations provides that network facilities and information systems operated or managed by the following units are included within the scope of protection for KII, if the destruction or experiencing a loss of functionality or data leakage with request to

[1] Please see our client alert for more details here.
[2] Please see our client alert for more details here.

such network facilities and information systems may severely jeopardize national security, the national economy and the people's livelihoods or the public interest:

- government agencies, and units in the fields of energy, finance, transportation, water conservancy, healthcare, education, social security, environmental protection, public utilities and other industries and sectors
- telecoms networks, broadcasting networks, Internet and other such information networks; and units providing cloud computing, big data, and other large-scale public information network services
- scientific research institutes and manufacturers in the fields of national defence science, technology and industry, large-scale equipment, chemical engineering, food and drugs and other such industries
- broadcasting stations, television stations, news agencies and other such press outlets
- other important units.

Compared with Article 31 of the Cyber Security Law[3] , the newly-added industries now considered to constitute KII are "national defence-related science, technology and industries, large-scale equipment, chemical engineering and food and drugs", while other additions can be seen as the refinement of existing industry categories. For instance, the "healthcare, education, social security, environmental protection and public utilities" industries may be seen as elaboration on the theme of the "public services" industry. The "telecoms networks, broadcasting networks, internet, providers of cloud computing, big data, and other large-scale public information network services, broadcasting stations, television stations, and news agencies" industries may be viewed as elaboration on the theme of the "public communications and information services" industry.

The Draft Regulations follow the two-step methodology for determining what constitutes a KII operator under the Cyber Security Law, which is to:

- first verify whether an enterprise falls under the list of specified industries
- then apply the test of potential hazardous consequences.

Furthermore, the catch-all phrase of "other important units" is tagged on at the end of the list, which means the category can be expanded at will by CAC officials, thereby removing any semblance of finality and definitiveness.

Article 19 of the Draft Regulations goes on to explain that the CAC, in conjunction with the relevant competent telecoms department, public security organs and so forth will formulate guidelines for identifying KII. This indicates that although Article 18 provides some basis for identifying which companies may be KII, ultimately whether a specific network facility or information system will be deemed a KII will be determined based on certain to-be-issued guidelines. This may presage the deployment of the results of the nationwide network security investigations and enquiries carried out since July 2016, where a set of internal Guidelines for Key Information Infrastructure Identification ("**Guidelines**")[4] were developed and used by the local authorities to conduct surveys on certain enterprises in China. The Guidelines divide KII into three categories:

- websites, such as websites of the Communist Party and government organs, enterprises

[3] Under Article 31 of the Cyber Security Law, the State must, on the basis of the cyber security protection system classification, implement key protections for public communications and information services, energy, transportation, water conservancy, finance, public services, e-government affairs and other such major industries and sectors, as well as other KII that may jeopardize national security, the national economy and the people's livelihoods or the public interest were it to be destroyed, or experience a loss of functionality or data leakage. The detailed scope of key information infrastructure and security protection measures for KII shall be formulated by the State Council.

[4] The Guidelines for KII Identification used in national security inspections were never officially issued by the CAC, but were available online.

and public institutions, as well as news websites

- platforms, such as Internet service platforms including instant messaging, online shopping, online payments, search engines, E-mail, BBS, maps, and audio/video
- production and business-related infrastructures, such as office and business systems, industrial control systems, large data centers, cloud computing platforms, and television relay systems.

Further, the Guidelines provide a chart listing key industries and set out a three-step process to identify KII operators:

- identify critical industries (including, for example, financial services and telecoms and Internet services)
- identify information systems or industrial control systems related to critical businesses
- identify a KII based on different materiality thresholds (including, for example, number of users, data volume and influence if damaged) applicable to the abovementioned three types of KIIs (i.e. websites, platforms and production and business-related infrastructures).

The Guidelines were widely believed to provide a foretaste of what is to come when they appeared on the Internet, but were never formally promulgated.

Further expansion of existing requirements for data localization and purchases of network products and services

Among other things, the most controversial requirements under the Cyber Security Law are:

- the data localization requirement and security assessment on cross-border transfers of personal information and important data due to operational needs
- the security review for purchases of network products and services by KII operators which may have an impact on national security.

The above two requirements are also elaborated on in the Draft Regulations in relation to KII.

Similar to the Cyber Security Law, the Draft Regulations restate that KII operators must store personal information and important data collected and generated during the course of their operations within China. Where, due to operational needs, it is truly necessary to send such information or data overseas, an assessment must be carried out in accordance with the Security Assessment Measures. Where laws or administrative regulations provide otherwise, such provisions shall apply.

Furthermore, in a new twist, Article 34 of the Draft Regulations requires that the operational maintenance of KII must be carried out within China. Where, due to operational needs, it is truly necessary to carry out remote maintenance from overseas, the matter must be reported in advance to the competent industrial supervisory authorities/regulatory agencies of the State and the public security department under the State Council. This raises the issue of whether such arrangements will be permitted going forward. No specific approval is mentioned, but it is only a stone's throw away from the authorities simply determining such arrangements are not acceptable in the interests of national security. Where global contracts are in place, having separate local maintenance will have cost and security implications.

As to the purchase of network products and services by KII operators, the Draft Regulations restate that where KII operators wish to purchase network products and services:

- if they involve key network equipment and specialized cyber security products, then such purchases must conform to laws and administrative regulations, as well as the mandatory requirements under the relevant

national standards (such as the KII Equipment First Batch)

– if such products or services may potentially have an impact on national security, such purchases must undergo a cyber security review under the Security Review Measures, and a security confidentiality agreement must be signed with the relevant product or service provider.

Furthermore, Articles 32 and 33 of the Draft Regulations require KII operators to conduct a security review of systems or software developed by outsourcing, and a security review of network products obtained through donation before such systems, software or products become operational and available. The latter seems to be almost anticipating attempts to sidestep the legislation. Moreover, upon the discovery of any security defects, vulnerabilities and other such risks during the use of network products or services, KII operators must take immediate measures to eliminate any risks and/or hidden hazards; and major risks involved must be reported to the relevant authorities. Nowhere is there any mention of the cost of addressing such requirements being borne by the Chinese state. It is one thing to hold a State-owned Enterprise to this standard, but quite another to hold a privately-owned Foreign-invested Enterprise ("**FIE**") to the same standard, against a background of rocketing labour costs in China.

Security protection obligations of KII operators

With respect to security protection obligations, the Draft Regulations reiterate requirements under the Cyber Security Law:

– Article 23 of the Draft Regulations is in essence a reworking of Article 21 of the Cyber Security Law, where it sets out general requirements applicable to all network operators to perform the security protection obligations based on the classification protection system

– Article 24 of the Draft Regulations is in essence a reproduction of Article 34 of the Cyber Security Law, where it sets out a set of special mandatory requirements for KII operators in relation to the designation, training and assessment of cyber security personnel, the backup plans and remedial measures, emergency response contingency plans and so forth.

In addition to repeating the requirements under the Cyber Security Law, the Draft Regulations also provide that:

– the principal person in charge of a KII operator is the primary person responsible for KII security protection work, and is accountable overall for KII security and protection within his/her organization

– the chief network security administrator of a KII operator shall take charge of the formulation and supervision of internal systems and operating procedures on cyber security, the formulation and supervision of internal rules on education and training plans, skill assessments of employees in key positions, cyber security investigation and emergency response drills, and the reporting of cyber security matters and incidents

– specialized cyber security technicians within a KII operator in key positions must have obtained certain qualifications before taking up such positions, and detailed rules on an employment certification system will be formulated; query how easy it will be for non-Chinese nationals to obtain such qualifications and the costs associated with such positions and qualifications appear to fall squarely on the shoulders of the employer

– in addition to the annual inspection and evaluation of security and potential risks as required under Article 38 of the Cyber Security Law, KII operators must establish

sound KII security testing and assessment systems, and conduct such security testing and assessments prior to going into operation or upon undergoing a major change.

Moreover, in addition to repeating the monitoring, advance warning and information reporting systems concerning cyber security under the Cyber Security Law to be established by the CAC and various governmental authorities, the Draft Regulations introduce random inspections and testing with respect to KII security risks and the performance of KII operators' security protection obligations on a regular basis. During such inspection and testing, KII operators may be required to provide statements from relevant personnel, provide access to and photocopies of documents/records, provide relevant internal regulations, allow the use of testing tools or permit cyber security service provider to carry out technical tests. Multinational enterprises may be alarmed at what type of information will be requested by such inspectors and whether their trade secrets will be at risk, not to mention the cost in money and business interruption terms.

Conclusions

The Draft Regulations, together with the other Supporting Legislation, on one level at least may have filled out some of the gaps in the cybersecurity legal framework in China, but in filling in the blanks left under the Cyber Security Law, the Draft Regulations have created new holes and introduced new uncertainties awaiting further legislation, namely the long-awaited guidelines for identifying KIIs, the rules related to qualifications of key personnel of KII operators, as well as the specific rules setting out the relevant requirements for institutions that:

– provide security testing and assessment for KII
– release information regarding security threats
– provide cloud computing and information technology outsourcing services aimed at KII.

It is not possible to reach any other conclusion than the fact that China's legal regime for cyber security protection is becoming increasingly onerous, costly, and potentially disruptive to business. Operators in the relevant industries are facing new compliance challenges each time a new piece of legislation is added to the list, and still do not know definitively what their obligations are. With regard to the specific scope of KII, the Cyber Security Law left the answer to be provided in the Draft Regulations, and now the Draft Regulations have left business waiting for a set of future guidelines to determine who is a KII. This is the legislative equivalent of 'kicking the can down the road', and is incredibly frustrating. Above all, the cost of compliance with the ever-growing laundry list of requirements looks to become even more prohibitive for those in the KII "bucket".

All in all, any sense of proportion appears to have been lost, with the legislators seeming to endlessly add more and more obligations onto the list without regard to the cost or business impact. For FIEs that are designated as KII, it would appear to send a clear message that national security concerns take precedence over the ability to operate a business without interruption from government authorities, and little regard seems to have been paid to the need to maintain a reasonable business cost base in China. There is no indication that any government help will be available to defray part of the cost, and so we seem to be moving in any unfortunate direction where cyber security compliance becomes a de facto trade barrier, by disincentivising foreign investment in any of the (newly-expanded) list of industries which may now be designated as KII.[5]

[5] See Article 35 of the Draft Regulations.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com