HAN KUN LAW OFFICES

Legal Commentary

CHINA PRACTICE • GLOBAL VISION

July 18, 2017

CII, Core Cybersecurity Law System Issued

David TANG | Min ZHU | Jundong GUO | Effy SUN

On July 10, 2017, the Cyberspace Administration of China ("**CAC**") promulgated the *Regulations on the Security Protection of Critical Information Infrastructure (Draft for Comment)* ("**Draft Regulations**"), which will be open for public comment until August 10, 2017.

As a supporting measure to the recently promulgated *Cybersecurity Law of the People's Republic of China* (the "**Cybersecurity Law**"), the Draft Regulations further detail the rules under Article 31 "Critical Information Infrastructure (**"CII"**)," which is of great significance for many enterprises in many industries. The Draft Regulations were drafted by the CAC and will ultimately be promulgated in the form of State Council regulations, which will place it in a higher position than other Cybersecurity Law supporting measures, which have generally been introduced in the form of departmental rules or recommended state standards.

General trends

Although the Draft Regulations was listed as the last "research project" on the 2016 State Council Legislative Program, many supporting measures and regulations have been issued by the CAC and others to implement the Cybersecurity Law since it was adopted on November 7, 2016 and came into effect on June 1, 2017, such as the *State Cybersecurity Emergency Response Plan* (January 10, 2017)*, Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad (Draft for Comment)* (April 11, 2017), *Network Product and Service Security Review Measures (Trial)* (May 2, 2017) and the *Catalogue of Critical Network Equipment and Special Network Security Products (First Batch)* (June 1, 2017). Until the issuance of the Draft Regulations, the fast pace at which the supporting measures have been issued shows both the urgent need and determination on the part of the government to implement the Cybersecurity Law and its supporting measures.

Main contents

The Draft Regulations reflect the government's intent to strengthen supervision and governance of CII, which is mainly reflected in the following:

a. The government will provide special support to guarantee CII security

The Cybersecurity Law sets forth generally that the government will support and promote cybersecurity. The Draft Regulations further stipulate that:

i. the government will formulate special industry, taxation, finance and talent policies in order to promote the development of CII security-related technologies, products, service innovation, personnel training, etc.;

ii. the government above the prefectural level will incorporate CII protection into the overall local economic and social development plan and will carry out performance evaluations of CII protection;

iii. the regulatory and supervision departments for various sectors will develop cybersecurity programs for their respective sectors and will establish and implement a working expense guarantee system;

iv. the energy, telecommunications and transportation industries are to be primarily responsible for providing support and protection with respect to the CII cybersecurity emergency response and the network function recovery, and the public security departments will combat relevant criminal activities in accordance with law.

Although the above provisions only set forth general principles related to CII protection, they impose compulsory obligations on relevant subjects by stipulating relevant subjects "shall" undertake certain responsibilities. This tone reflects the government's determination to guarantee CII protection and its intent to strictly regulate this sector.

b. Further expanding the definition of CII

Similar to the Cybersecurity Law, the Draft Regulations define CII by giving a non-exhaustive list of named industries. However, the coverage scope of CII under the Draft Regulations has clearly been expanded compared to the Cybersecurity Law.

In addition to the seven important industries or areas listed in the Cybersecurity Law, the Draft Regulations set forth that information infrastructure used in the healthcare, education, environmental protection, national defense, science and technology, large-scale equipment, chemical, food and medicine and news industries, as well as information infrastructure used to provide large public information network services such as cloud computing and big data services should also be regarded as CII. Specifically, CII operators include:

i. Government organizations and energy, finance, transportation, water resources, healthcare, education, social security, environmental protection and public utility industry units;

ii. Information networks such as telecommunications networks, radio and television networks and the Internet, as well as units providing cloud computing, big data and other large public information network services;

iii. Scientific research and production units in the industries of national defense, science and technology, large-scale equipment, chemicals and food and drugs, etc.;

iv. News units such as radio stations, television stations, news agencies, etc.;

v. Other key units.

In addition to industries and sectors listed above, Article 19 of the Draft Regulations stipulate that CAC and other regulatory departments will later jointly formulate and promulgate the CII identification guidelines, according to which the regulatory or supervision departments of various industries identify CIIs in their respective sectors and will report such findings.

Although further detailed rules such as the identification guidelines have not yet been promulgated, enterprises in the industries and sectors listed in the Draft Regulations should be sufficiently aware of developments in this area and make advance preparations. Currently, we recommend such enterprises to preliminarily determine whether their business may be regarded as a CII by referring to the *National Network Security Inspection and Operation Guidelines,* promulgated in June 2016, through considering the full nature of industries to which their business belongs, the level of dependence on the network facilities or information systems, and the influence of security risks related to the network facilities or information systems that they operate, which are assessed on a "qualitative + quantitative" basis.

c. Strengthened obligations and accountability mechanisms

In addition to the security protection obligations applicable to general network operators and CII operators as provided in the Cybersecurity Law, the Draft Regulations further clarify the obligations and responsibilities of relevant natural persons:

i. Clarifies that the person in charge of the CII operator is the primary responsible person for the CII security protection within the unit, and who shall be responsible for establishing and implementing the corresponding security responsibility systems and assumes full responsibility related to enterprise operations (Article 22);

ii. Appointment of specialist cybersecurity managers (Article 25);

iii. Professional and technical personnel at key positions are to acquire a license to be employed and should receive cybersecurity education and training at least 3 working days each year (Articles 26 and 27);

iv. Employees are to receive at least 1 working day of cybersecurity education and training each year (Article 27).

One major characteristic of the Draft Regulations is to significantly the strengthen liability of natural persons. Almost all provisions under Chapter 7, "Legal Liability," stipulate that, in case of violations, penalties are to be imposed on both the violating enterprise and the natural persons in charge of the enterprise. This is consistent with the recent regulatory practice of holding the relevant individuals in charge also liable for an enterprise's illegal conduct, especially by stipulating that the persons in charge of CII operators are to be the primarily responsible for CII security protection. Enterprises potentially subject to these rules and their management are advised to pay sufficient attention to this issue.

In addition, Article 51 of the Draft Regulations also provides associated liability for CII operators, third-party professional service organizations and the relevant departments in cases of severe cybersecurity incidents in which such parties are found to be liable. Thus, if a cybersecurity incident occurs, relevant cybersecurity service organizations and departments may also be subject to legal liability if the incident is caused due to their dereliction of duty, malfeasance or other violations.

d. Product and service outsourcing and CII operations and maintenance subject to stricter requirements

Similar to the Cybersecurity Law, the Draft Regulations categorize network products and services purchased or used by CII into general network products and services and key network equipment and special network security products. CII operators must carry out security supervision of products and services that they purchase or use in accordance with the Cybersecurity Law, the *Network Product and Service Security Review Measures (Trial)* and *Catalogue of Critical Network Equipment and Special Network Security Products (First Batch)* and follow-up catalogues. Specifically, the Draft Regulations require:

i. Systems and software developed through outsourcing, as well as donated network products are subject to security examinations before being put into use (Article 31);

ii. Operation and maintenance of CIIs is to be carried out within the territory of China. Reports should be made in advance to the competent department or the supervisory department and the public security department if offshore remote maintenance is determined to be necessary (Article 34);

iii. "Agencies providing CII-related services, such as security monitoring and evaluation, security threat information issuances such as information regarding system vulnerabilities, computer viruses and network attacks and services of cloud computing and information technology outsourcing" is to conform to specific requirements jointly developed by CAC and the State Council (Article 35).

In particular, the following points require special attention:

i. the Draft Regulations strengthen regulations over third-party professional service providers by requiring that third-party providers obtain certain qualifications to provide CII-related services, which echoes the third-party liability investigation mechanism as described above;

ii. based on the CII data localization and export security assessment requirements, the Draft Regulations further stipulate that CIIs are subject to "domestic operation and maintenance," which will undoubtedly have an enormous impact on compliance efforts by multinationals that engage in cross-border business cooperation and technical support (both within the group and externally).

Advice for enterprises

The Draft Regulations expand the definition of CII and further clarify the management requirements and obligations of CII operators based upon the Cybersecurity Law. However, generally speaking, the Draft Regulations are only a framework document related to CII security protection and a significant number of issues still remain to be refined and clarified.

The promulgation of the Draft Regulations is regarded as an important step for the implementation of CII key and systematic supervision. We expect other CII security protection-related supporting measures and guidelines to be developed and promulgated in the future, including the *Critical Information Infrastructure Identification Guidelines*, provisions related to CII testing and evaluation requirements and procedures, licenses required to be obtained by professional and technical personnel to serve in key cybersecurity positions, and qualifications to be obtained by agencies to provide CII-related services.

However, this does not mean that enterprises can adopt a wait-and-see approach. Instead, relevant enterprises, especially those belonging to the industries and areas specified in the Draft Regulations, should conduct a review and self-examination of their network security and data compliance status as soon as possible in accordance with existing laws, regulations and safety standards, such as the Cybersecurity Law and its supporting documents and documents referenced in the Draft Regulations. The content of such examinations would include reviewing job responsibility management, performance of network security protection obligations, data usage and storage status, as well as the security of purchased network

products and services. Where necessary, enterprises should seek assistance from technical, legal and other professionals. In addition, enterprises should also maintain close, active communications with industry regulators and supervisors and closely observe developments in cybersecurity-related policies, especially the latest policy developments related to CII.

Han Kun Cybersecurity and Data Compliance Series:

I : Big Data Policy and Legal Issues in the Healthcare Industry

II : Comments on the Network Security Law

III: Comments on the Measures on Security Assessments for Personal Information and Important Data to be Transmitted Abroad (for Public Comment)

IV: The Unveiling of Cybersecurity Reviews

V : Personal Information Protection from the Perspective of Criminal Law

VI: Guidelines on Data Export Security Assessments

● 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.

Should you have any questions regarding this publication, please contact **Mr. David TANG （+8621-6080 0905; david.tang@hankunlaw.com ） or Mr. Min ZHU （ +8621-6080 0955; min.zhu@hankunlaw.com）.**