NEWSLETTER
LIFANG & PARTNERS 立方观评

No.48
2017.07

SPECIAL ISSUE

THE LEGAL FRAMEWORK FOR CYBERSECURITY IN CHINA

THE LEGAL FRAMEWORK FOR CYBERSECURITY IN CHINA

The Cybersecurity Law that came into effect on 1st June 2017 addresses issues of cybersecurity, along with data security, privacy protection and network security. It is a milestone in the regulation of online activities in China due to its width and depth.

In this article, we will briefly address key points in the laws that regulate cybersecurity in China. At the time of writing this, there are the following important laws, regulations, measures and guidelines, enacted or drafted for public comments:

1. **The Cybersecurity Law** effective on 1st June 2017

2. **The Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)** released on 11th April 2017 for public consultation

3. **Measures on Security Examination for Online Products and Services (Trial Implementation)** released by CAC and effective on 1st June 2017

4. **Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)** released by the National Information Security Standardization Technical Committee on 27th May 2017

5. **Catalogue of Critical Network Equipment and Specialized Cybersecurity Products (First Batch)** released and effective on 1st June 2017

6. **The Regulations for the Security Protection of Critical Information Infrastructure (Exposure Draft)** released by CAC for public comment on 10th July 2017.

I The Cybersecurity Law

This law was effective on 1st June 2017. It contains 79 articles, broken into 7 chapters and may be divided into the following themes:

1. Introduction, purpose, goals, principles, administration and definitions (Chapters 1, 2 and 7);

2. Networks and information security (Chapters 3 and 4);

3. Monitoring, early warning and emergency response (Chapter 5); and

4. Legal liabilities (Chapter 6).

Introduction, purpose, goals, principles, administration and definitions: The purpose of the Cybersecurity Law is to ensure cybersecurity, cyberspace sovereignty, national security, public interests, protect the rights and interests of citizens, legal persons and others, and promote the healthy development of IT in economic and social sectors.

The Cyberspace Administration of China (CAC) is responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration. The authority in charge of telecommunication, the public security authority and other relevant authorities of the State Council shall, ex officio, take charge of protection, supervision and administration of cybersecurity pursuant to the present Law and applicable laws and administrative regulations.

Networks and information security: For most businesses the most important concepts to understand in regards to this theme of the Cybersecurity Law are:

A. General Obligations of Network Operators;

B. General Obligations of Providers of Network Products or Services;

C. Special Obligations of Critical Information Infrastructure Operators;

D. Personal Information; and

E. Security Examinations and Assessments.

We shall now discuss each of these themes in turn.

A. The general obligations of network operators are to:

(1) Formulate internal security management systems and operation instructions;

(2) Take technical measures to protect cybersecurity;

(3) Take technical measures to monitor and record network operation and cybersecurity events, and maintaining those records for no less than six months;

(4) Take such measures as data classification, and backup and encrypt of important data, etc.; and

(5) Perform other obligations provided for in relevant laws and administrative regulations.

B. General Obligations of Providers of Network Products or Services: The providers of network products or services must not use malware, must provide consistent security maintenance, obtain consent for collecting personal information and comply with certain product standards. Additionally, providers of network services, but not providers of network products, fall within the category of network operators.

C. Special Obligations of Critical Information Infrastructure Operators

(1) Critical Information Infrastructure: Critical Information Infrastructure (CII) is described in Article 31 of the Cybersecurity law as:

... critical information infrastructure in important industries and sectors such as public communications, information service, energy, transport, water conservancy, finance, public service and e-government, and other critical information infrastructure that, once damaged, disabled or data disclosed, may severely threaten the national security, national economy, people's livelihood and public interests...

CII can be defined both in terms of industries and the results of security breaches.

Industries have been clearly listed, while results include threats to national security, the national economy, people's livelihoods and public interest.

(2) In addition to general obligations of network operators, the operator of a critical information infrastructure shall also take care to:

1) Set up a dedicated security management body and designate a person in charge, and review the security backgrounds of the said person and those in key positions;

2) Provide employees with regular cybersecurity education, technical training and skill assessment;

3) Make disaster recovery backup of important systems and databases;

4) Work out an emergency plan for cybersecurity events and carry out drills regularly; and

5) Perform other obligations provided for in relevant laws and administrative regulations.

(3) Limitation on cross border data transfer

Article 37 of the law states:

The operator of a critical information infrastructure shall store within the territory of the People's Republic of China personal information and important data collected and generated during its operation within the territory of the People's Republic of China. Where such information and data have to be provided abroad for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail.

CII operators who have generated and collected personal and important data in China should store that data in China. Personal and important data may be transferred out of China only if necessary and following a security assessment.

D. Personal Information: Personal information may only be collected where "lawful, justifiable and necessary."

Personal Information is defined as "various information which is recorded in electronic or any other form and used alone or in combination with other

information to recognize the identity of a natural person, including but not limited to name, date of birth, ID number, personal biological identification information, address and telephone number of the natural person." (Art. 76)

Monitoring, Early Warning and Emergency Response: These obligations generally apply to the CAC who must prepare for and monitor cybersecurity threats, conduct threat assessments, conduct cybersecurity drills and provide public warnings.

Legal Liabilities: Violation of the Cybersecurity Law may result in fines ranging from RMB 5,000 to 1 million, imprisonment, and being banned from holding key posts related to cybersecurity and network operation. Prohibited acts include:

- Failure to take steps to ensure a network is free from interference, disruption or unauthorised access, and prevent data disclosure, theft or tampering;
- Failure to develop emergency plans for cybersecurity events and promptly respond to risks;
- Using products that do not satisfy the mandatory requirements of national standards or using malware;
- Failure to obtain users' identity information;
- Failure to conduct cybersecurity authentication, tests, risk assessments, and to release cybersecurity information such as system bugs, computer virus, network attack and intrusion;
- Threatening cybersecurity, providing programs or tools for such activity, or providing assistance for any such activity; and
- Infringing upon any right in personal information that is legally protected.

Prohibitions that only apply to CII network operators include:

- Failure to take steps to ensure steady continuous operations;
- Failure to create a dedicated network security department staffed by qualified people with a designated leader;
- Failure to provide network security staff with continuing professional development;
- Failure to ensure adequate data backups are in place;

- Failure to make emergency plans and carry out regular emergency drills;
- Failure to ensure that security and confidentiality obligations apply to network product or service providers;
- Failure to conduct annual reviews and submit them to the government; and
- Failure to perform anything else required by law.

II The Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)

These draft measures were released on 11th April 2017 for public consultation. They contain 18 Articles in total.

The draft provides a definition of "important data" and some guidelines for cross-border transfer of important data and personal information, including prior notification and consent, and Security assessments.

Important data is defined as data closely related to national security, economic development, and social and public interests. Further national standards are planned to further define this concept.

The security assessment for data to be transmitted abroad should consider:

(1) Necessity of the transfer;

(2) Personal information involved including if consent is given;

(3) Important data involved;

(4) How safe the information will be at its destination;

(5) Risks of leakage, damage, alteration and abuse of data after being transmitted;

(6) Risks to national security, social and public interests, and personal interests; and

(7) Other important matters.

In certain circumstances, the security assessment must be carried out by an industry regulator. Such circumstances include:

(1) The data contains in total the personal information of more than 500,000 users;

(2) The quantity of the data is more than 1,000 gigabytes;

(3) There is data related to nuclear facilities, chemical biology, defence industry, population and health, large-scale project activities, marine environment and sensitive geographic information;

(4) The data contains system vulnerabilities, security protection or CII information;

(5) A CII operator provides personal information and important data abroad; or

(6) Other data that may affect national security, social and public interests, oris necessary for assessment as determined by a regulator.

If there is no definite regulator, the CAC shall organise the assessment and complete it within 60 working days.

Data shall not be transmitted abroad in any of the following circumstances:

(1) The transmission abroad is not authorised by the data subject or may jeopardise personal interests;

(2) The transmission may affect national security and jeopardise social and public interests; or

(3) Other data forbidden by the authorities.

These measures are only in draft form at this stage. They give an insight into what the regulators are currently considering.

III Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)

The National Information Security Standardization Technical Committee released the draft guidelines on 27th May 2017 allowing a month for public comments. The draft guidelines apply to network operators conducting security assessments and regulatory authorities supervising those network operators.

Network operators, who export important data or personal information abroad, must formulate data export plans. Such plans should include:

1. The destination, scope, type and scale of the data export;

2. The information systems involved;

3. Any transit country or region;

4. Destination risks; and

5. Security control measures.

Specific assessment methods to identify important data and to review plans are suggested. In such, the guidelines provide much reference to important concepts and procedures relating to the implementation of the Cybersecurity Law.

IV Measures on Security Examination for Online Products and Services (Trial Implementation)

On 1st June 2017, the Measures on Security Examination for Online Products and Services (Trial Implementation) came into effect. The purpose of these measures is to promote controllable security levels for online products and services, prevent cyber security risks, and to safeguard national security.

These measures contain 16 articles in total.

Examination Circumstances: Cyber security examinations will be triggered when important online products and services are purchased by network and information systems involving national security. They will also be triggered when online products and services are purchased by key industries.

Examination Points:

Cyber security examination shall focus on examination of security and controllability of online products and services, which shall mainly include:

(1) Inherent security risks of products and services, as well as the risks of illegal control or interference and disrupted operation;

(2) the supply chain security risks;

(3) the risks of products and services providers making use of the facilitating conditions for provision of products and services to collect, store, process and use user-related information illegally;

(4) the risks of product and service providers making use of users' reliance on products and services, and thus compromising cyber security and user interests; and

(5) any other risks which may compromise national security.

Examination Organization: Relevant governmental bodies will jointly create a Cyber

Security Examination Committee who will issue examination policies, coordinate significant issues and implement examinations.

The Cyber Security Examination Committee will form a Cyber Security Examination Expert Panel to carry out third party evaluations of the security risks of online products and services and the security and credibility of their providers.

Third Party Organizations: The third party cyber security examination agencies recognized by the State pursuant to the law shall undertake the third party evaluation work in cyber security examination.

The third party agencies should adhere to the principles of objectivity, equitableness and fairness, and comply with the law and relevant standards. They will be held responsible for the results of their examinations.

Key Industries: The regulatory authorities for certain key industries will be responsible for organizing and conducting examinations within their industries. Those industries are public communications and information services, energy, transport, water resources, financial, public services and government e-services etc.

Reporting Obligations: Product and service providers are responsible for cooperating in cyber security examination work and the truthfulness of materials they provide. The entities involved with examinations shall keep any information reviewed as confidential and only use it for examination purposes. The Internet Security Examination Office shall release reports of products and services on an ad hoc basis.

Product or service providers who feel that they have not been treated objectively and equitably or that their information has not been kept confidential may lodge a report with the Internet Security Examination Office or the relevant authorities.

Violations: Violation will be dealt with pursuant to the Cybersecurity Law.

V Catalogue of Critical Network Equipment and Specialized Cybersecurity Products (First Batch)

This catalogue is the result of provisions within the Cybersecurity Law that requires providers of network products or services to comply with certain standards for their products. The catalogue was prepared jointly by several government authorities, including the CAC, the Ministry of Industry and Information Technology, the Public Security Bureau, and the Certification and Accreditation Administration and it was effective since 1th Jun, 2017. Products listed in the catalogue must be examined by a

qualified institution before being supplied.

VI The Regulations for the Security Protection of Critical Information Infrastructure (Exposure Draft)

These regulations, which were made available for public comment on 10th July 2017, have the express purpose of ensuring the security of critical information infrastructure. In total, they consist of 55 articles, broken into 8 chapters. The following key points may be of interest:

A. General Principles and Prohibitions: Of particular note are the prohibitions. Prohibitions include:

(1) Attack, intrude, disturb or damage critical information infrastructure;

(2) Illegally obtain, sell or provide to others without authorization any technical data or other information that may be used specifically to endanger critical information infrastructure;

(3) Conduct any scanning detection of penetration or attack nature on critical information infrastructure without authorization;

(4) Be fully aware that a person engages in activities that endanger the security of CII, but still provide the person with internet access, server hosting, network storage, communication, advertising and marketing, payment and settlement or any other service; and

(5) Engage in other activities endangering CII.

B. Critical Information Infrastructure: As you may recall, CII can be defined in the Cybersecurity Law by reference to certain industries or results. These measures further specify industries that are CII as follows:

(1) Government agencies and entities in the energy, finance, transportation, water conservation, health care, education, social insurance, environmental protection and public utilities sector;

(2) Information networks, such as telecommunication networks, broadcast television networks and the internet, and entities providing cloud computing, big data and other large-scale public information network services;

(3) Research and manufacturing entities in sectors such as science and technology for national defence, large equipment manufacturing, chemical industry and food and drug sectors;

(4) Press units such as broadcasting stations, television stations and news agencies; and

(5) Other key entities.

C. Operators' Duties: Operators of critical information infrastructure are responsible for the security of critical information infrastructure and must protect cybersecurity, accept government supervision and be socially responsible.

Operator obligations that have not previously been mentioned include:

- The designated person in charge of cybersecurity must:

(1) Organise the formulation of the cybersecurity system and operational rules, and supervise their implementation;

(2) Organise the skill assessments forkey position holders;

(3) Organise the delivery of cybersecurity training;

(4) Organise cybersecurity inspections, emergency rehearsals and resolve incidents; and

(5) Report key cybersecurity matters and events to the authorities.

- Establish and improve a security inspection and evaluation system for CII. Security inspections and evaluations shall be conducted prior to the operation of CII or when a major change occurs.

- Operators of CII must organise one staff training day per year.

D. Governmental Obligations: Whilst most of this section repeats what is mentioned elsewhere, the specific powers of authorities to make random inspections on CII are detailed. During random inspections authorities may do the following:

(1) Request relevant personnel to explain inspection and assessment matters;

(2) Access, retrieve, copy and protect the information relating to security protection;

(3) Examine the formulation and implementation of cybersecurity management systems, as well as the planning, construction and operation of cybersecurity technical measures;

(4) Use testing tools or entrust a third party agency to carry out technical testing; and

(5) Other necessary approaches agreed by operators.

Advice

The legal framework for Cybersecurity in China is growing and becoming progressively more complicated. Because of the wide application of the cybersecurity laws, network service and product providers should do their best to comply with the law.

---------- **By Lifang Cybersecurity Law Team**

IMPORTANT INFORMATION

This Newsletter has been prepared for clients and professional associates of Lifang & Partners. 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.

For more information, please visit our website at www.lifanglaw.com. If you have any questions, please contact us at info@lifanglaw.com or

Beijing Office

Address	Room 1105, Tower A, Nan Xin Cang International Building, No.A22, Dongsishitiao Street, Dongcheng District, Beijing, P.R.China 100007
Telephone	(86-10) 64096099
Fax	(86-10) 64096260,64096261

Guangzhou Office

Address	Room 3806, Building G, G.T.Land Plaza, No. 16, Zhujiang East Road, Zhujiang New Town, Tianhe District, Guangzhou P. R. China
Telephone	(86-20)85561566, 85561660, 38898535
Fax	(86-20)38690070

Wuhan Office

Address	Room 1002, Tower C, Han Street Headquarter International, No.171 Zhongbei Road, Wuchang Dist, Wuhan, Hubei, P. R. China
Telephone	(86-27) 87301677
Fax	(86-27) 86652877

Seoul Office

Address	Guanghuamun Officia Building 1416 , Saemunan-ro 92 , Jongno-gu, Seoul Republic of Korea
Telephone	+0082 02 69590780