The 2016 China Cybersecurity Law Summary

CDS Global Cloud

https://www.cdsglobalcloud.com

China’s New Cybersecurity Law
Revised July 2016

Background Info

The first draft of the Cybersecurity Law was released in July 2015. On July 5, 2016, China’s National People’s Congress (“NPC”) published a revision of the Cybersecurity Law for public comment. The revised draft contains several significant changes, but many of the provisions from the first draft that raised concerns among multinational companies, especially those in the tech sector, remain. The new Cybersecurity Law means strict new rules for foreign corporations doing business in China and has the potential to discriminate against foreign technologies in favor of domestic industry.

What and who it effects:

- Network product and service providers, operators*: These companies are now required to censor any information deemed ‘critical’ or ‘banned’ and demand real name registration for any user of services like instant messaging.
- All personal information for citizens in China and any business data deemed ‘important’ must be stored on storage devices inside mainland China. The terms are vague enough to apply to a wide variety industries and a wide range of data. Any data transmitted outside of China by any entity must first be reviewed and approved.
- All network transmissions must be monitored and "network security incidents" are required to be reported. The company, service provider, or operator is then required to give "technical support" to help in an investigation. This support might result in authority’s access to internal or external communications, etc.
- The new law also states that no individual will be allowed to use the Internet to endanger national security, promote terrorism, spread false information to disturb the economic order, etc. This regulation is very open-ended and may be interpreted to fit a multitude of situations.

Click here for a summary of China’s new Cybersecurity Law and Critical Information Infrastructure

Click here for a complete translation of China’s new Cybersecurity Law by the American Chamber of Commerce – China

The primary challenge issued by the new Cybersecurity Law is the requirement that data be stored in mainland China and the standard practice of foreign companies to centralize their IT infrastructure outside of mainland China. Building a redundant IT infrastructure in China is not practical, and it isn't feasible to “move everything to China."

If this is your dilemma, CDS has the solution. We can provide an easy to deploy, low impact, and fully legitimate solution. ***Contact us for a free consultation.***

Summary: Articles most impactful to foreign companies

The six primary directives:

1. **Clarify the cyberspace sovereignty principle;**
2. **Clarify the security obligation of network product and service providers;**
3. **Clarify the security obligations of network product and service operators*;**
4. **Further, improve personal information protection rule;**
5. **Establish the Critical Information Infrastructure security protection system;**
6. **Establish the cross-border data transmission rules of important data on Critical Information Infrastructure.**

1. Article 15: Network Products

The State establishes and revises network security standards. The State Council Administrative Department for Standardization and other relevant State Council departments organized the formulation and revision of pertinent national and industry standards for network security management as well as for the security of network products, services, and operations.

Pay close attention to the network product standard issued by each department.

2. Article 37: Personal and important business data stored in mainland China

Personal information and other important business data gathered or produced by Critical Information Infrastructure operators during operations within the mainland territory of the People's Republic of China shall be stored within mainland China. When business requirements it is necessary to transmit data outside the mainland, the measures jointly formulated by the State Network Information departments and the relevant departments of the State Council requiring a security assessment shall be followed unless laws and/or administrative regulations provide otherwise in which case they shall take precedence. This provision establishes the following three specific principles:

(1) Principle of the cross-border restriction of personal information

Personal information and other important business data gathered by Critical Information Infrastructure operators during operations within the mainland territory of the People’s Republic of China are subject to the sovereignty of the People’s Republic of China. In other words, personal information and important business data falls not only under the scope of civil property or commercial assets but also are subject to the rules of sovereignty regulation.

(2) Server domestication principle

Article 37 places great emphasis on the storage of information and data within the territory, requiring any server containing personal information and data considered to be critical must be located within the territory of the People's Republic of China. Although the information may be transmitted globally, the relevant operators will legally be responsible for the storage of the information and data on storage devices physically located in China.

(3) Principles for the review of cross-border flow of critical information and data
When business requirements it is necessary to transmit data outside the mainland, the measures jointly formulated by the State Network Information departments and the relevant departments of the State Council requiring a security assessment shall be followed unless laws and/or administrative regulations provide otherwise in which case they shall take precedence.

3. **Article 35: Countermeasures of trans-national enterprises**

(1) Pay close attention to the list of " Critical Information Infrastructure" operators*.
Article 35 of the "Cybersecurity Law" restricts the "Critical Information Infrastructure”. In Article 31 The State implements the fundamental protection of public communication and information services, power, traffic, water, finance, public services, electronic governance, and other Critical Information Infrastructures that if destroyed, lose function, or leak data might seriously endanger national security, national welfare, the people’s livelihood, or the public interest on a tiered protection system.
The State Council will formulate the specific scope and security protection measures for Critical Information Infrastructure. Accordingly, the network operator should be concerned about the relevant rules of the State Council and judge if the customer is subject to the Critical Information Infrastructure operators to determine whether to adapt to the restrictions of Article 35.
(2) Adhere to the requirement of physical storage in mainland China
Storage devices containing personal information or important data and their backup storage devices must strictly adhere to the requirement that the physical storage location is in mainland China. Also, the data must be isolated physically from any associated foreign servers and/or storage devices.
(3) Establish a rigid internal data security management system
For information or data brought into the control scope of Chinese cyberspace sovereignty, strict data security management and data transmission control systems must be implemented. Any interior person is strictly forbidden to perform data transmission until the relevant department's safety assessment is completed.

The National Cybersecurity Law went into effect on June 1st, 2016. Although we understand that the primary infrastructures affected by this law are the designated "Critical Information Infrastructures," the State Council has not yet published an official guideline clearly defining the criteria determining a **Critical Information Infrastructure.**

However, the attached information adapted from the regional guideline, *Critical Information Infrastructure Determination Guide*, from the Cybersecurity and Information Safety Office of ShiZuiShan City can be used as a reference until a more definitive guideline is published.

**The translated term ‘operators' is vague and includes companies across all industries, not just those limited to the data center or telecom providers.*

Below is a partial translation of the Cybersecurity Law:

1.What is Critical Information Infrastructure?

Critical Information Infrastructure refers to information systems or industrial control systems which provide network information services or support the operation of important industries such as energy, communication, finance, traffic, and public utilities. Systems, that if destroyed, might seriously endanger the normal operation of vital industries and/or result in severe disruption to national politics, the economy, science and technology concerns, national defense, social or cultural traditions, the environment and/or people’s livelihood.

The Critical Information Infrastructure includes: website categories (e.g. websites of party and government institutions, enterprise, institutions, and news sites), platform categories (e.g. instant messaging, online shopping, online payments, search engines, e-mail, forums, GPS maps, audio and video, etc.), network service platforms, production business categories (e.g. office and business systems, industrial control systems, large data centers, cloud computing platforms, and television relay systems, etc.).

2. How to Identify Critical Information Infrastructure

The identification of Critical Information Infrastructures usually involves three steps:

1. Identification of critical services
2. Identification of information systems or industrial control systems supporting mission-critical services
3. Identification based on the degree of dependency of critical services on the information or industrial control system and the resultant loss(es) caused by a network security incident.

(1). Identify the mission-critical services for a designated area, department or industry.

The following table is a reference to industries and departments determined to be mission-critical services. It is not intended to be a complete listing.

Industry		Critical service
Energy Source	Electric Power	• Power generation (including thermal power, hydroelectric power, and nuclear power, etc.) • Power transmission • Electric power distribution
	Oil and Gas Industry	• Oil and gas exploration • Refining and processing • Oil and gas transportation • Oil and gas storage
	Coal	• Coal mining • Coal chemical industry
Finance		• Bank operations • Securities and futures trading • Liquidation payment • Insurance operations
Traffic	Railway	• Passenger services • Freight services • Transportation production • Station operations
	Civil Aviation	• Air traffic control • Airport operation • Booking, departure, and flight control arrangements • Airline Operations
	Highway	• Traffic regulation • Computerized transportation systems (one-card-pass, ETC charge, etc.)
	Maritime Transportation	• Any maritime transportation operations (including passenger transport and freight service) • Port management operations • Shipping traffic control

Water Conservation	• Operation and control of water conservation • Long distance water delivery controls • Urban water resource controls
Medical and Health	• Operations of health agencies such as hospitals • Disease control • Operations of emergency aid centers
Environmental Protection	• Environmental monitoring and early warning systems (water, air, soil, nuclear radiation, etc.)
Industrial Manufacturing (Raw materials, equipment, consumer goods, electronic manufacturing)	• Enterprise operations and management • Computerized manufacturing systems (Industrial Internet, Internet of Things, intelligent equipment, etc.) • Production, processing, and storage control of hazardous chemicals (chemical, nuclear, etc.) • Operations controlling high-risk industrial facilities
Municipal Services	• Water, heating and gas supply management • Urban rail transit • Sewage treatment • Operations and control of smart cities
Telecommunication and the Internet	• Voice, data, and Internet infrastructure and hubs • Domain name resolution services and national top-level domain registration management • Data center/cloud service
Television and Radio Broadcasting	TV and Radio broadcast controls Broadcast controls

Governmental Departments	• Information disclosure • Public service departments • Office business systems

(2). Identification of information systems or industrial control systems supporting mission-critical services

Information systems or industrial control systems supporting a critical service operation or related to a critical service should be listed per the critical service to formulate a list of possible Critical Information Infrastructures (e.g. generator control systems and management information systems for thermal power enterprises in Energy Sources; the water works production control systems and water supply network monitoring systems involved in Municipal Water.

(3) Confirm the Critical Information Infrastructure

For information systems or industrial control systems listed as candidates for Critical Information Infrastructure, the final declaration of status is determined by the industry standards of that region, department, and industry.

A. Website category

Those websites meeting one or more of the following conditions qualify as a Critical Information Infrastructure;

1. Web sites of the party and/or government offices at county level (included) or above
2. Key news websites
3. Web sites with a daily visit of more than 1 million
4. In the event of a network security incident websites which meet the following criteria:

(1) Influence the work and lives of greater than 1 million people

(2) Influence the work or lives of more than 30% of the population in a single prefecture-level city

(3) Result in the disclosure of personal information of greater than 1 million individuals

(4) Result in the disclosure of sensitive information from institutions and enterprises

(5) Result in the disclosure of data regarding national geography, population, and/or resources, etc.

(6) Seriously damage the government’s image, the social order, or endanger national security.

5. Any other websites that should be identified as Critical Information Infrastructure.

B. Platform category

Those meeting one or more of the following conditions should be identified as Critical Information Infrastructure;

1. The number of registered users exceeds 10 million or the number of active users (which log in at least once a day) exceeds 1 million
2. The average daily number of orders or transactions is greater than RMB ¥10 million (approximately USD $1.4 million).
3. In the event of a network security incident any platform which meet the following criteria:
    (1) Result in greater than ¥10 million (approximately USD $1.4 million) in a direct economic loss
    (2) Directly influence the work and lives of greater than 10 million people
    (3) Result in the disclosure of personal information of greater than 1 million individuals
    (4) Result in the disclosure of sensitive information from institutions and enterprises
    (5) Result in the disclosure of data regarding national geography, population, and/or resources, etc.
    (6) Seriously damage the government's image, the social order, or endanger national security
4. Any other websites that should be identified as Critical Information Infrastructure.

C. Production service category

Those meeting one or more of the following conditions should be identified as Critical Information Infrastructure:

1. Public service operational systems of offices above the prefecture-level city, or any urban management systems related to medical treatment, security, firefighting, emergency command, production dispatch or traffic command, etc.
2. Data centers having greater than 1500 standard racks
3. In the event of a network security incident any platform which meet the following criteria:
    (1) Influence the work or lives of greater than 30% of the population in a single prefecture-level city
    (2) Influence the water, power, or gas utilization, the oil consumption, the heating and/or the traffic of 100 thousand people or more
    (3) Result in greater than five deaths or more than 50 severely injured individuals
    (4) Result in greater than RMB ¥50 million (approximately USD $7 million) in direct economic loss;

(5) Result in the disclosure of personal information of greater than 1 million individuals

(6) Result in the disclosure of sensitive information from institutions and enterprises

(7) Result in the disclosure of data regarding national geography, population, and/or resources, etc.

(8) Seriously damage the government's image, the social order, or endanger national security

4. Any other websites that should be identified as Critical Information Infrastructure.

For more information or if you have questions, please contact us.

Web:	CDSGlobalCloud.com
Tel:	888.826.3476
Email:	Sales@CDSGlobalCloud.com

CDS Global Cloud

10000 N Central Expressway Ste 400

Dallas, TX 75231