ROPES & GRAY

ALERT

Privacy & Data Security

July 7, 2017

An In-Depth Examination of China's New Cybersecurity Law Part I: Who Must Comply?

Attorneys
Cori A. Lable
Heather Egan Sussman
Michael Xiao
David Chen

On June 1, 2017, China's new cybersecurity law, the *Network Security Law of the Peoples Republic China* ("*Cybersecurity Law*") went into effect. The *Cybersecurity Law* contains an overarching framework regulating network products, equipment, and services, as well as the operation and maintenance of information networks, the protection of personal information, and the supervision and administration of cybersecurity in China. The new law is in line with other major governments releasing laws and orders designed to promote cybersecurity of essential services and critical infrastructure. In Europe, for example, the European Commission enacted on July 6, 2016, a directive on the security of network and information systems (the "NIS Directive"),[1] directing EU member states to identify essential services, establish appropriate security measures and notify relevant national authorities of serious incidents. In the United States, President Trump signed on May 11, 2017 an Executive Order directing federal departments and agencies to adopt security controls based on an established cybersecurity framework and support cybersecurity efforts of critical infrastructure entities.[2]

Criticism has followed the new *Cybersecurity Law* since its announcement in 2016, due to its many unclear provisions and broadly defined terms, which, given the ubiquitous use of data networks by companies today, means the law could potentially apply to – and significantly impact operations of – a large swath of companies of all types and sizes with a footprint in China. In addition, several related regulations published by the Cyberspace Administration of China ("CAC") went into effect at the same time as the *Cybersecurity Law*.[3] The regulation known as the *Measures on the Security Assessment for Personal Information and Important Data to be Transmitted Abroad* ("*Draft Data Transfer Measures*") has been most widely discussed given its potential impact on the free flow of data. While the *Draft Data Transfer Measures* had been slated to come into effect at the same time as the *Cybersecurity Law*, a press release issued by the CAC on May 31, 2017 reports that it will now be further reviewed and amended over the next 12 months.[4]

While some commentary has been published on certain aspects of the *Cybersecurity Law*, including on its data localization requirements and consent requirements, this two-part series will examine issues that do not appear to have been examined in depth: Part I will examine which entities are regulated and which Chinese government bodies regulate them, taking a close look at how the new law has defined the important categories of "Network Operators", "Critical Information Infrastructure" and "Critical Information Infrastructure Operators"; Part II will take an in-depth look at data security assessments and transmission of data across Chinese borders under the *Cybersecurity Law*.

---

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194).
[2] Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 11, 2017).
[3] Other relevant CAC regulations that went into effect on June 1, 2017 will not be discussed in detail in this article and include: *Internet Information and Content Management Administrative Enforcement Procedures*, *Network Products and Services Security Review Method (Trial)*, and *Internet News Information Service Management Regulations. (all translations unofficial)*
[4] *See* China Internet Information Office Officials Answer Reporter's Questions Prior to the Implementation of the Cybersecurity Law (translated) (May 31, 2017), available as of June 19, 2017 at http://www.cac.gov.cn/2017-05/31/c_1121062481.htm. The Draft Data Transfer Measures were first released for comment in April 11, 2017, and then updated on May 19, 2017.

A. The Relevant Regulators

Both the *Cybersecurity Law* and the *Draft Data Transfer Measures* expressly state that the "national cyberspace authority" will have a central role in the planning, coordination, supervision, and management of network security measures.[5] This "national cyberspace authority" is generally understood to be the CAC. Although the CAC – also known as the Office of the Central Leading Group for Cyberspace Affairs – is less than four years old (founded in 2014), it serves as China's central agency in the oversight of internet and network related affairs, and has become one of the most important arms of the Chinese central government. The CAC answers directly to the Central Leading Group for Internet Security and Informatization, which is led by President XI Jin Ping and consists of China's top officials.

Other than the CAC, the national authority for telecommunications, the public security bureau, and other relevant but unspecified authorities are in charge of network security protection, supervision and management within the scope of their responsibilities.[6]

Under the Cybersecurity Law, critical information infrastructure operators are required to perform a security assessment when transferring personal information across Chinese borders. The Draft Data Transfer Measures expand the scope of who is required to conduct such security assessments to all network operators, and provides that industry regulators will be responsible for overseeing such security assessments within their respective sectors. Thus, although the CAC is the highest-level body when it comes to China's new cybersecurity rules, primary supervision of cross-border assessments will likely be governed by industry-specific reviews. Enforcement and oversight of the new requirements therefore will likely involve a multi-agency effort, depending on the particular business activities and industries implicated. However, part of the burden of complying with China's new cybersecurity rules will fall on businesses themselves as part of their obligation to conduct their own security assessments under the Draft Data Transfer Measures. Key to understanding the scope and provisions of the new law, we discuss the definitions of "critical information infrastructure operators" and "network operators" further below.

B. Organizations Subject to the Cybersecurity Law's Regulations

The *Cybersecurity Law* has broad potential applicability and may impact to varying degrees a wide array of industries beyond traditional technology, telecommunication and internet companies.

1. ***Network Operators***

The *Cybersecurity Law* expressly applies to two groups of entities. The first is "Network Operators", which is defined as "owners, operators, and service providers of networks."[7] This definition covers not just IT-related companies, but may also be broadly interpreted to encompass all businesses and organizations that operate a network of computer terminals and/or data storage units in China, including, for example, businesses and organizations that operate their own internal or external computer networks in China or that operate their own websites in China. Many small-, medium-, and large-sized Chinese companies and multinational companies with some network capabilities in China may therefore be considered a "Network Operator" under the *Cybersecurity Law* and subject to its regulation. Companies that operate networks to provide services or conduct business activities or to store personal information of customers or personnel are likely to be covered.

[5] *Cybersecurity Law*, Article 8; *Data Transfer Measures*, Article 5.
[6] *Cybersecurity Law*, Article 8.
[7] *Cybersecurity Law*, Article 76(3). "Network" refers to "systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing." *Cybersecurity Law*, Article 76(1).

2. ***Critical Information Infrastructure Operators***

The second group which the law applies to is CII Operators, which is a subset of Network Operators. CII Operators are subject to notably stricter requirements than Network Operators, which warrants a closer examination of the category's boundaries. However, the definition of CII Operators is not clearly defined in the *Cybersecurity Law*. Article 31 of the *Cybersecurity Law* provides a non-exhaustive list of critical information infrastructure by reference to the following industry sectors: public communication, information services, energy, transportation, water, finance, public services, and e-government. By listing these industry sectors, the *Cybersecurity Law* appears to be implying that these industry sectors are those that have or are likely to have critical information infrastructure. Article 31 also contains a catch-all provision that includes other important industry sectors and critical information infrastructure loss of which would cause serious damage to national security, the economy, people's livelihood, or public interest (listed industry sectors and catchall provision are together referred to herein as the "*Article 31 Categories*").[8]

Industries that may contain critical information infrastructure

It should be emphasized that the Article 31 Categories are non-exhaustive and are sufficiently broad to cover a wide range of specific industries and sectors that may be considered to have critical information infrastructure. The CAC has discussed in other documents additional (or perhaps more specific) industries that may be considered to have critical information infrastructure. These documents include:

- *National Network Security Inspection Operational Guide ("Operational Guide")*, published in June 2016, which identifies specific industries and sub-industries, and then further breaks them down into specific types of businesses within those industries and sub-industries (*discussed further in the next section*);[9]
- *The National Cyberspace Security Strategy ("Security Strategy")* published on Dec. 27, 2016, which lists "healthcare, scientific research, industrial manufacturing, and social welfare" when discussing industries with critical information infrastructure;[10] and
- *First (consultation) draft of the Cybersecurity Law*, published on July 6, 2015, which lists "television broadcasting" and "healthcare care and hygiene" as specific examples of industries with critical information infrastructure.

As a result, we expect that industries and sectors expressly mentioned in other CAC documents likely will be deemed to fall under one of the *Article 31 Categories*, or under Article 31's catch-all provision as industries that may be considered to have critical information infrastructure. Furthermore, as explained below, a business or organization that operates in an industry or sector not expressly discussed by the CAC still faces a risk that some aspect of its operations may have critical information infrastructure.

Operations that may have critical information infrastructure

The *Cybersecurity Law* does not address the question of whether an entity will be deemed a CII Operator solely because it operates in an industry or sector that expressly or implicitly falls within Article 31 of the *Cybersecurity Law* or other related CAC regulations. For this issue, however, the *Operational Guide* provides some much needed guidance. In particular, the *Operational Guide* first sorts critical information infrastructure into three types:

- "website type", such as government and political party websites, enterprise websites, news websites;
- "platform type", such as instant messaging, online shopping, online payment, search engines, email, forums, maps, audio and video, and other network service platforms; and

[8] *Cybersecurity Law*, Article 31.
[9] *Operational Guide*, Section 3.2.
[10] *Security Strategy*, Article 4(3).

- "production business type", such as office and operations systems, industrial control systems, big data center, cloud computing platforms, television broadcasting systems.

The *Operational Guide* then outlines three steps to determine what constitutes critical information infrastructure:

Step 1: The first step is to determine the "key businesses" within each region, department, and industry. Unlike the scant details in the *Cybersecurity Law*, the *Operational Guide* includes a "Critical Information Infrastructure Operations Business Assessment Table"[11] ("*Assessment Table*") which lists the relevant industries and key businesses that may contain critical information infrastructure. While there does not appear to be an official English translation of the contents of the table, we provide an unofficial translation of the *Assessment Table* as follows.

Industry		**Key Businesses**
Energy	Power	Power generation (including thermal power, hydro power, nuclear power, etc.)
		Power transmission
		Power distribution
	Petroleum and Petrochemical	Oil and gas exploration
		Refinery and Processing
		Oil and gas transport
		Oil and gas storage
	Coal	Coal mining
		Chemical processing of coal
Finance		Banking operations
		Securities and future trading
		Liquidation payment
		Insurance operations
Transportation	Rail	Passenger service
		Freight service
		Transport production
		Station operations

[11] *Operational Guide*, Table 1, Section 3.2

	Civil Aviation	Air traffic control
		Airport operations
		Ticket reservation, departure and flight scheduling inspection arrangements
		Airline operations
	Roads	Road traffic control
		Intelligent traffic systems (all access cards, ETC tolls, etc.)
	Water transport	Water transport Water transport company operations (including passenger service and freight service)
		Port management and operations
		Shipping traffic control
Water conservancy		Water conservancy hub operations and control
		Long distance water supply control
		City water source control
Healthcare and hygiene		Hospital and healthcare institution operations
		Disease control
		Emergency center operations
Environmental protection		Environmental observation and monitoring (water, air, soil, nuclear radiation, etc.)
Industrial manufacturing (raw materials, equipment, consumer goods, electronics manufacturing)		Enterprise operations management
		Intelligence manufacturing systems (industrial internet, internet of things, intelligent equipment, etc.)
		Hazardous chemicals production, processing, and storage control (chemicals, nuclear, etc.)
		High risk industrial facilities operations and control
Municipal		Water, heat, gas supply management
		urban rail transport

	Wastewater management
	Intelligent city operations and control
Telecommunications and the internet	Voice, data, internet infrastructural network and hubs
	Domain name analytical services and national top level domain registration management
	Data centers /cloud services
Radio and television	Television broadcasting control
	Radio broadcasting control
Government departments	Information disclosure
	Public-facing services
	Office operations systems

Step 2: The second step is to determine the "information systems" or "industrial control systems" that are relevant to the key businesses. According to the *Operational Guide*, these are systems that ensure the functioning of the key businesses, or that are related to the key businesses. Examples of such systems provided by the *Operational Guide* include management information systems of thermal power operators and monitoring systems of water supply networks.

Step 3: The third step is to see if the information systems or industrial control systems of the key businesses contain or use one of the three types of critical information infrastructure ("website type", "platform type", or "production operations type") and whether such infrastructure meets or exceeds certain quantitative and qualitative criteria or thresholds. If they do, then such key businesses with such information systems or industrial control systems may be identified as having critical information infrastructure. The *Operational Table* lists the specific quantitative and qualitative criteria and thresholds used to evaluate the "three types" of critical information infrastructure discussed earlier ("website type", "platform type", "production operations type"). Again, due to the lack of official English translation, we provide an unofficial translation as follows.

Website Type	Websites of party and government organs that are of county-level or above
	Important news websites
	Websites that generates over 1 million views on a daily basis
	In the event of an network safety incident, may cause one of the following: • Affect the lives or work of over 1 million people • Affect the lives or work of over 30% of the population within a single city-level administrative area • Cause the leak of personal information of over 1 million people

	• Cause the leak of a large quantity of sensitive information of organizations or institutions • Cause the leaks of a large quantity of geography, population, resources or other national infrastructural data • Severely damage governmental image, social order, or endanger national security
	Others that should be identified as critical information infrastructure
Platform Type	Over10 million registered users, or over 1 million active (at least 1 login a day) users
	Daily completed order amount or transaction amount of over 10 million RMB
	In the event of an network safety incident, may cause one of the following: • Cause over 10 million RMB in direct economic loss • Directly affect the lives or work of over 10 million people • Cause the leak of personal information of over 1 million people • Cause the leak of a large quantity of sensitive information of organizations or institutions • Cause the leaks of a large quantity of geography, population, resources or other national infrastructural data • Severely damage governmental image, social order, or endanger national security
	Others that should be identified as critical information infrastructure
Production Operations Type	Operational systems of city-level or above government organs that are for public facing services, or city management systems that are related to healthcare, security, fire control, emergency command, production scheduling, traffic control, and others
	Data centers with over 1,500 standard workstations
	In the event of an network safety incident, may cause one of the following: • Affect the lives or work of over 30% of the population within a single city-level administrative area • Affect the water usage, power usage, gas usage, petro usage, heating, or transportation of over 100,000 people • Result in deaths of more than 5 people or serious injuries to more than 50 people • Directly cause over 50 million RMB in economic loss • Cause the leak of personal information of over 1 million people • Cause the leak of a large quantity of sensitive information of organizations or institutions • Cause the leaks of a large quantity of geography, population, resources or other national infrastructural data

	• Severely damage governmental image, social order, or endanger national security
	Others that should be identified as critical information infrastructure

If a business or organization and its operations or systems or parts thereof satisfy the three steps above, then that business or organization and its operations or systems may be identified as having critical information infrastructure under the *Operational Guide* and, accordingly, that entity may be considered a CII Operator under the *Cybersecurity Law*.

One additional important note - the *Operational Guide* is intended to be used as a reference when districts, departments, and organizations carry out network safety inspections on critical information infrastructure. Therefore, while its level of specificity is certainly helpful from a practical perspective, it does not have the same legal force as the *Cybersecurity Law* or even other CAC regulations. Businesses should thus be cautious not to draw definitive conclusions about whether its operations or systems contain critical information infrastructure based solely on the *Operational Guide*, pending further guidance from CAC or specific advice from local Chinese counsel.

C. Key Takeaways

After considering the *Cybersecurity Law*, the *Operational Guide*, and other relevant CAC regulations, a few takeaways may be reasonably drawn.

1. As briefly noted above, the *Article 31 Categories* likely implicitly include industries and sectors discussed in other CAC documents related to the *Cybersecurity Law* and its implementation, including the *Operational Guide* and the *Security Strategy*. It is likely that the drafters of the *Cybersecurity Law* have intentionally kept the language broad in order to allow the CAC or other relevant regulators to specify the relevant industries and sectors through regulations and other guidance.
2. Not all operations or systems of businesses or organizations under the *Article 31 Categories* are automatically considered as critical information infrastructure. That is, certain operations or system of such a business or organization may be ruled out using the three-part test of the Operational Guide. Using a bank as an example, the bank's data regarding stock trading operations may be considered as critical information infrastructure by meeting the three-step test. On the other hand, the bank's internal expenditures data (e.g. travel costs, office rental, employee salary etc.) may not be considered as critical information infrastructure if it fails any step of the three-step test.
3. A business or organization may not automatically be considered a CII Operator solely on operating in an industry or sector that expressly or implicitly falls under the *Article 31 Categories*. Rather, when the *Cybersecurity Law* is read in combination with the *Operational Guide*, it appears that a business or organization would at least need to have some critical information infrastructure in order to be considered a CII Operator. Using a telephone manufacturer as example, while telephones are related to public communications, it might be unreasonable to treat a telephone manufacturer as a CII Operator simply because its operations have some relevance to public communications.
4. For businesses whose primary businesses do not appear to fall under the *Article 31 Categories*, it is possible – though with a lower likelihood -- that some aspects of its operations would nonetheless be considered as having critical information infrastructure. One possibility is that the business or some part of its operations gets snagged under Article 31's catchall provision. Another possibility is if a business has secondary operations or internal operations that happen to touch upon one of the *Article 31 Categories* (or the catch-all provision), and satisfy the three-step test under the *Operational Guide*. For example, an automotive manufacturer may collect extensive data regarding road traffic controls or intelligent traffic systems, perhaps for its internal knowledge management or business strategy purposes. Unknowingly, this automotive manufacturer may have become owners of transport related critical information infrastructure.

5. It remains unclear whether a business or organization would be treated as a CII Operator because some aspect of its operations or its systems is deemed to be critical information infrastructure. On the one hand, it is fairly likely that, if a business' primary business or systems are considered critical information infrastructure, then the entire business or organization will be treated as a CII Operator. On the other hand, what if, similar to the example in point four, only a small part of a business' or organization's operations or systems are considered critical information infrastructure, and the remainder not? Absent added clarity on this issue, organizations in such situations might consider adopting a conservative approach and treating itself as a CII Operator until it is informed otherwise by legal counsel or the relevant regulatory authorities.

6. It also remains unclear whether the *Cybersecurity Law*'s and related regulations' requirements regarding CII Operators apply to that business or organization in the entirety, or only with respects to the elements of the business or organization that are considered critical information infrastructure. For example, the *Cybersecurity Law* states that any "Personal Information"[12] and "Important Data"[13] "gathered or produced by CII Operators during operations within mainland China should be stored within mainland China."[14] If a business is considered a CII Operator, does this requirement – often referred to as the data localization requirement – apply to all of the CII Operator's data? Or does it govern only personal information and important data related to the business' critical information infrastructure, but not other (non-critical) operations or systems? Again, absent added clarity from regulators or advice from Chinese local counsel, CII Operators with a mix of critical and non-critical information infrastructure might consider adopting a conservative approach and treating the relevant requirements as being applicable to all aspects of its operations and systems.

As the Chinese government will continue to revise its regulations and consider whether and how to release guidance on the *Cybersecurity Law*, companies are wise to consider these threshold scoping questions and determine whether the new law applies. In our next installment of this two-part series, we will discuss the substantive requirements of the *Cybersecurity Law*, and how impacted companies operating in China can address some of its more challenging aspects.

[12] "Personal information" refers to "all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth." *Cybersecurity Law*, Article 76(5).
[13] "Important data" is not defined in the Cybersecurity Law, but is defined in the *Draft Data Transfer Measures* as "data closely related to national security, economic development, and social and public interests." *Draft Data Transfer Measures*, Article 17.
[14] *Cybersecurity Law*, Article 37.