PAUL HASTINGS

STAY CURRENT

April 2017

Follow @Paul_Hastings

China's New Cybersecurity Regime

By Robert P. Silvers, Haiyan Tang, Steven D. Winegar, Behnam Dayanim, John Tso, & Minda Huang

With China's new *Cybersecurity Law* (网络安全法, "CSL") coming into effect on June 1, 2017, companies operating in China need to consider the major implications of this law and how to address compliance with what is a new and untested set of requirements.

The CSL and related guidance issued this year by the Cybersecurity Administration of China ("CAC") impose on a broad range of companies requirements to store data locally in China, to undergo an as-yet-undefined "security review" of certain IT infrastructure, and to implement prescriptive cybersecurity governance measures, among other mandates.

This client alert outlines the key points of China's new cybersecurity regime and concludes by proposing several action items for clients to prepare for the implementation of the applicable rules once the CSL takes effect.

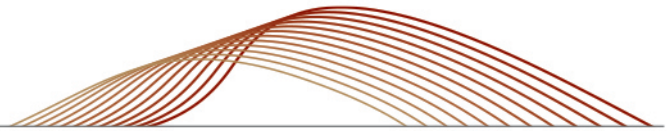
Scope and Application of the CSL

The CSL mainly regulates "Network Operators" (网络运营者) and "Critical Information Infrastructure Operators" (关键信息基础设施, "CII Operators"), and we describe the scope of these two important categories below, as well as the requirements applicable to each.

Network Operators

"Network Operators" are "network owners, administrators, or service providers,"[1] a broad definition that could be interpreted to cover any company using the Internet or other networks to conduct business. Accordingly, virtually every multinational company doing business in China may be deemed to come within the scope of the CSL and related mandates. Network Operators' obligations include:

- Formulating an internal security protocol and operating procedures, including the designation of specific corporate officers responsible for network security;
- Adopting technical measures to prevent and mitigate cyber intrusions;
- Making notifications to users and regulatory authorities upon identification of any security deficiency and loophole;
- Adopting technical measures to monitor and record the operating status of a network and security incidents, and preserving related network logs for at least six months; and
- Adopting such measures as data categorization, disaster recovery back-up of important data and systems, and encryption of important data.[2]



- Furthermore, Network Operators providing internet, phone, or messaging access to customers "shall require users to provide their real identity," and deny service to customers who refuse to do so.[3]

CII Operators

CII Operators are subject to additional requirements under the CSL. Critical Information Infrastructure ("CII") is defined broadly to cover enumerated industries, including public communication and information services, power, transportation, water, finance, public services, and e-government affairs, as well as a catch-all category of other infrastructure that "might seriously endanger national security, the national economy, people's livelihood, or the public interest" if such infrastructure is damaged, malfunctions, or experiences a data leak.[4] While the CSL states that the precise scope of CII will be specified at a later time by the State Council, prior regulatory guidance[5] in China contains a non-exhaustive list of the key businesses that are likely to be deemed to involve CII (see **Appendix A**).

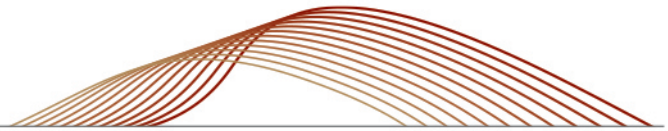
In addition to the requirements imposed on Network Operators, CII Operators are also subject to the following obligations:

- Establishing specialized security management departments and persons in charge, and conducting background checks of personnel in key security positions;[6]
- Conducting regular cybersecurity education, training, and skill assessment exercises for employees;[7]
- Carrying out disaster recovery backup of important systems and databases;[8]
- Formulating emergency response plans for cybersecurity incidents and conducting regular drills;[9]
- Undergoing state security assessments conducted by competent authorities when procuring network products or services "that may affect state security;"[10]
- Conducting, or engaging a qualified third party to conduct, annual cybersecurity and risk assessments, and submitting the assessment results and improvement plans to the competent authority;[11] and,
- Cooperating and sharing certain cybersecurity information with government authorities, relevant research institutions, and cybersecurity service institutions.[12]

Most significantly, the CSL stipulates that personal information and other important data collected in China by CII Operators are required to be stored domestically. Moreover, a security review by Chinese government authorities is required if a CII Operator wants to transfer such data outside of China.[13]

Data Localization and Out-of-China Data Transmission

On April 11, 2017, the CAC issued for public comment the *Security Assessment Measures regarding the Exit of Border of Personal Information and Important Data (Draft for Consultation)* (个人信息和重要数据出境安全评估办法（征求意见稿）, "Draft CAC Data Measures"), extending data-localization requirements to Network Operators, which by definition would cover CII Operators.[14] Under the original CSL, only CII Operators had been subject to the data localization requirements,[15] so this draft, if enacted in final form, would mark a significant broadening.



Under the Draft CAC Data Measures, if Network Operators have legitimate business needs to transmit personal information or important data outside China, they are required to undertake a security assessment.[16] The relevant factors under this assessment include the size, scope, type, and sensitivity of the data involved, and whether the transmission was consented to by the owner of the personal information.[17] Chinese government authorities must conduct the assessment (i.e., a corporate self-assessment is not sufficient) if the out-of-China transfer:

- involves the personal information of over 500,000 individuals;
- exceeds 1,000 GB;
- concerns nuclear facilities, chemistry and biology, national defense and military, public health, large-scale construction activities, the marine environment, or sensitive geographical data;
- concerns CII security issues; or
- involves data transmitted by CII operators.[18]

The Draft CAC Data Measures also contain a catch-all provision stating that the measures could be "of reference" when "other individuals and organizations" transmit personal information and important data collected and generated within China.[19] Thus, these requirements could in some instances impact the operations of non-Network Operators and non-CII Operators.

Proposed Action Items

With less than two months remaining before the effective date of the CSL, companies operating in China should consider taking the following actions:

Evaluating Whether the Company Comes Within the Scope of the New Requirements

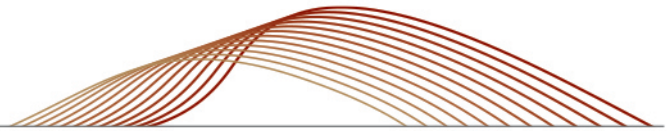
In light of the vague and potentially sweeping definitions of CII Operators and Network Operators, companies should evaluate immediately whether their operations put them within the law's scope. Companies should also understand whether any of their clients or customers in China could be considered CII Operators. Any purchase of network products or services by CII Operators that could affect state security is subject to state security inspection.[20] In addition, suppliers of such products and services are required to sign security and confidentiality agreements with CII Operators.[21]

Preparing to Store Personal Information and Important Data within China

Companies need to examine how they are storing and transferring data they collect and generate in China. The data localization and cross-border transfer requirements will have a significant impact on the way companies run their operations in China. With the law coming into effect on June 1 and the interpretation and enforcement landscape still unclear, impacted companies need to engage in data mapping and compliance policy reviews now.

Conducting Cybersecurity Governance and Policy Assessments

Companies should review and potentially update their internal cybersecurity and privacy policies and governance structures. The CSL will require many companies to have designated personnel in charge of cybersecurity; to have mechanisms for providing information upon request from law enforcement; to preserve certain cybersecurity network data for specified periods; to implement employee training programs; to have cyber incident response plans; and to conduct cybersecurity exercises. Companies that are likely to be classified as CII or Network Operators should take steps to ensure compliance before the law goes into effect.



Preparing for Government Security Reviews

The CSL requires security reviews of CII Operators, including the network equipment that CII Operators procure. The Chinese government has offered little guidance as to what these security reviews will entail, but we recommend that companies prepare for implementation of the law by reviewing which of their intellectual properties, trade secrets, source codes, or other sensitive information requires protection.

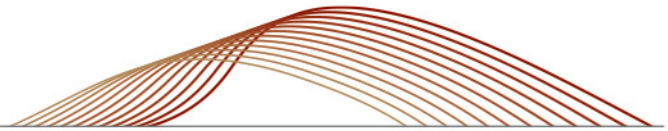
How Paul Hastings Can Help

Paul Hastings' Privacy and Cybersecurity practice can help companies prepare for the impending effective date of the CSL. Our team—based in the United States, Europe, and China—has been monitoring the law and is developing practical approaches that take into account the continuing uncertainty the law presents. One member of our team recently joined us from the United States government, where he engaged in direct discussions with representatives of the Chinese government regarding the CSL, affording us valuable insights into their objectives. In addition, we possess deep experience in helping enterprises in a variety of industries design multi-jurisdictional compliance programs that address differing legal requirements across national boundaries.

Appendix A

List of Major Industries and Businesses Deemed to Involve CII[22]

Industry		Key Business
Energy	Electricity	Electricity generation (thermal power, hydropower, nuclear power, etc.)
		Electricity transmission
		Electricity distribution
	Oil and petrochemical	Oil and gas exploitation
		Refining and processing
		Oil and gas transmission
		Oil and gas storage
	Coal	Coal mining
		Coal chemical industry
Finance		Bank operations
		Securities and futures transactions
		Settlement and payment
		Insurance operations
Transportation	Railway	Passenger services
		Freight services
		Transportation Operation
		Station operation
	Civil aviation	Air traffic control
		Airport operation
		Booking, departure, and flight scheduling



Industry		Key Business
		Airline operation
	Road	Road traffic control
		Smart transportation systems (smart card, ETC payment, etc.)
	Water transportation	Water transportation company operation (passenger service and freight service)
		Port operation management
		Shipping traffic control
Water resources		Operation and management of critical hydraulic facilities
		Operation and management of long-distance water supplies
		Operation and management of urban water sources
Medical and healthcare		Operation of healthcare institutions (including hospitals)
		Disease control
		Emergency rescue center operations
Environment protection		Environmental conditions monitoring and early warning systems (water, atmosphere, soil, nuclear radiation, etc.)
Industrial manufacturing (manufacture of raw materials, equipment, consumer goods, electronics)		Operation and management of manufacturing enterprises
		Smart manufacturing systems (industrial internet, Internet of things, smart equipment, etc.)
		Hazardous materials production, processing, and storage (chemical, nuclear, etc.)
		Operation and management of high-risk industrial facilities
Municipal facilities		Management of water, heat, and gas supplies
		Urban rail transportation
		Sewage treatment
		Operation and management of “smart cities” (智慧城市)
Telecommunications and the Internet		Basic network and hubs of voice, data, and the Internet
		Domain name resolution services and registration management of national top-level domain names
		Data center/cloud service
Broadcasting		TV broadcasting
		Radio broadcasting
Education		Information disclosure on websites of universities, colleges, secondary schools, and primary schools, and on schools’ intranet systems
		Teaching and research
News website		[Not specified]
Business platforms		Instant messaging, online shopping, online payment, search engines, email, forums, maps, audio and video, etc.

Industry	Key Business
Government authorities	Information disclosure
	Public service
	Operating systems

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Hong Kong

Steven D. Winegar
852.2867.9003
stevenwinegar@paulhastings.com

London

Ashley P. Winton
44.020.3023.5121
ashleywinton@paulhastings.com

New York

James H. Koenig
1.212.318.6005
jimkoenig@paulhastings.com

San Francisco

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Shanghai

Haiyan Tang
86.21.6103.2722
haiyantang@paulhastings.com

John Tso
86.21.6103.2942
johntso@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

[1] CSL art. 76.3.

[2] CSL art. 21. 22.

[3] CSL art. 24.

[4] CSL art. 31.

[5] E.g., *Work Plan for Cybersecurity Assessment of Critical Information Infrastructure* (关键信息基础设施网络安全检查工作方案) issued by the Tianjin CAC on June 24, 2016; *Notice on Provincial Cybersecurity Assessment of Critical Information Infrastructure* (关于开展全省关键信息基础设施网络安全检查的通知) issued by Liaoning CAC on August 8, 2016.

[6] CSL art. 34.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] CSL art. 35.

[11] CSL art. 38.

[12] CSL art. 39. The types and scope of the information to be shared have not been clarified at this point.

[13] CSL art. 37.

[14] Draft CAC Data Measures art. 2.

[15] CSL art. 37.

[16] Draft CAC Data Measures art. 9.

[17] Draft CAC Data Measures art. 8.

[18] Draft CAC Data Measures art. 9.

[19] Draft CAC Data Measures arts. 16.

[20] CSL art. 35.

[21] CSL art. 36.

[22] Included in several cybersecurity assessment guidelines issued by provincial CACs to their local counterparts, *see* footnote no. 4. Translation for reference only.