JONES DAY | One Firm Worldwide℠

WHITE PAPER

August 2017

Implementing China's Cybersecurity Law

China's Cybersecurity Law came into effect on June 1, 2017. Three months later, many uncertainties remain as only some of the anticipated implementing regulations have been issued. However, based on draft and final regulations and guidance that have been issued to date, there are a number of steps that companies should take now to comply with and prepare for anticipated compliance obligations.

TABLE OF CONTENTS

China's Cybersecurity Law was issued on November 7, 2016, by the Standing Committee of the National People's Congress, and it came into effect on June 1, 2017. The Cybersecurity Law marks the first comprehensive law in China specifically regulating cybersecurity.

The Cybersecurity Law contains detailed requirements that covered entities must meet, and it imposes significant legal liabilities for companies that breach its provisions. However, there are still many uncertainties regarding its operation and enforcement in practice, as several anticipated implementing regulations are yet to be formally issued. Notwithstanding these uncertainties, China has already started bringing enforcement actions against companies for violations of the Cybersecurity Law. Given the evolving cybersecurity landscape, companies operating in or collecting data from China should prioritize compliance and continue to monitor China's new Cybersecurity Law and corresponding regulations.

This *White Paper* addresses what is known and what is anticipated for companies seeking to comply with the Cybersecurity Law.

KEY CONCEPTS

Who Must Comply with the Cybersecurity Law?

The Cybersecurity Law applies primarily to network operators, critical information infrastructure ("CII") operators, and providers of network products and services. As a first step, businesses operating in China should carefully assess whether they could fall within one or more of these categories.

"Network Operators" are broadly defined as those that own or manage networks or that provide network services (Article 76). This could be deemed to include anyone that operates his or her own IT network or provides online services in China. So far, there is no indication that the authorities will adopt a narrower definition.

"CII Operators" are a subset of Network Operators that own or manage CII, which include businesses that operate in the following sectors:

- Public communications and information services;
- Energy;
- Transportation;
- Water conservancy;
- Finance; and
- Public services and e-government affairs.

Other businesses may be considered CII Operators if they have infrastructure that would seriously endanger national security or the economy, people's livelihood, or the public interest. According to the *Draft Regulation on the Protection of Critical Information Infrastructure* ("Draft CII Protection Regulation") circulated for public comment on July 10, 2017, such businesses may include:

- Government organizations and entities in the industries or fields of energy, finance, transportation, water conservancy, health, education, social security, environmental protection, and public utilities;
- Information networks such as telecommunications networks, radio and television networks, and the internet, and entities providing cloud computing, big data, and other large-scale public information network services;
- Scientific research and production entities in industries such as national defense, heavy equipment, chemicals, and food and drugs; and
- News entities, such as radio stations, television stations, and news services.

Neither the Cybersecurity Law nor any related regulation—draft or final—defines "network products" or "network services," but, based on the interpretation of other similar terms, businesses should assume that any product or service that could fall within these terms based on a broad definition is likely to do so. For the purposes of this *White Paper*, we have referred to providers of network products or services collectively as "Network Providers."

Personal Information and Important Data

The Cybersecurity Law imposes a number of obligations on Network Operators with respect to personal information and important data.

Under the Cybersecurity Law, "personal information" means any 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 full names, birth dates, identification numbers, personal biometric

information, addresses, and telephone numbers (hereinafter "Personal Information").

The Judicial Interpretation on Several Issues on the Application of Law in Handling Criminal Cases of Infringement of Personal Information of Others 2017, which was issued by the Supreme People's Court and the Supreme People's Procuratorate on May 9, 2017, and came into effect on June 1, 2017, effectively expanded the definition of "personal information" in the Cybersecurity Law to include all information reflecting a natural person's activities.

The definition and scope of "important data"—omitted from the Cybersecurity Law—is described in detail in the *Draft Measures for the Security Assessment of Outbound Transmission of Personal Information and Important Data and the Information Security Technology—Guidelines for Cross-Border Data Transfer Security Assessment* (discussed below).

OBLIGATIONS AND LIABILITIES UNDER THE CYBERSECURITY LAW

The Cybersecurity Law sets out:

- General obligations of all Network Operators;
- Additional obligations that apply to CII Operators;
- Obligations of Network Providers; and
- Legal liabilities and government powers.

General Obligations of All Network Operators

All Network Operators are required to comply with the following obligations (Articles 21, 24-26, 28, 42, and 47 of the Cybersecurity Law):

- Develop internal security management rules and operating procedures;
- Identify person(s) in charge of cybersecurity;
- Implement technical measures to prevent computer viruses, network attacks, network intrusions, and other acts endangering cybersecurity (measures may include firewalls, intrusion detection, and a mitigation and recovery plan);
- Implement technical measures to monitor and record the status of network operations and cybersecurity incidents, and preserve relevant weblogs for not less than six months;
- Categorize all data collected;
- Back up and encrypt all "important data";
- Require users to provide true identity information when Network Operators provide network access, domain name registration, access services for fixed-line or mobile phone, information publishing service, or instant message service, and further require Network Operators to refuse to provide such services to any user who fails to do so;
- Make and immediately initiate emergency response plans for cybersecurity incidents, take corresponding remedial measures, and report cybersecurity incidents to the competent department when they occur;
- Remedy system bugs, computer viruses, network attacks, network intrusions, and other security risks in a timely manner;
- Provide technical support and assistance to public security and national security authorities to safeguard state security and investigate crimes;
- Follow the relevant laws and regulations in conducting cybersecurity authentication, testing, and risk assessments;
- Notify the public, in accordance with applicable regulations, regarding cybersecurity information on system bugs, computer viruses, network attacks, and network intrusions;
- Immediately cease releasing or transmitting information that is prohibited by law or administrative regulation, and take necessary measures to handle or delete such unlawful information, prevent it from spreading, preserve any relevant records, and report the prohibited release or transmission to the competent department;
- Undertake any steps required by the Cybersecurity Law to protect users' information; and
- Perform other obligations as prescribed by law and administrative regulation.

Additional Obligations of CII Operators

In addition to the obligations imposed on all Network Operators, under Articles 34-38 of the Cybersecurity Law, CII Operators are required to:

- Establish special security management institutions, designate persons in charge of security management, and conduct security background checks on designated

individual(s) in charge of security management and any personnel in key positions;
- Conduct cybersecurity education, technical training, and skill assessment for employees on a periodic basis;
- Make disaster recovery backups of important systems and databases;
- Make emergency response plans for cybersecurity incidents and organize drills on a periodic basis;
- Enter into security and confidentiality agreements with Network Providers to specify obligations and responsibilities when purchasing network products or services;
- Detect and assess cybersecurity positions and potential risks (or entrust cybersecurity service institutions to do so) at least once a year and submit detection and assessment reports and identified improvement measures to the relevant department in charge of the security protection of CII; and
- Obtain prior approval of security review organized by the Cybersecurity Administration of China ("CAC") in conjunction with other relevant regulators when purchasing network products or services that may affect national security.

Obligations of Network Providers

Network Providers should comply with relevant national standards and mandatory requirements. This might include, for example, complying with the *Self-Disciplinary Convention on the Network Copyright on the Internet of China 2001*, which requires Network Providers to oversee users' dissemination of information on websites; timely delete harmful information; observe relevant intellectual property protection rules when producing, distributing, or disseminating network information; guide users toward using the network in a civilized manner; strengthen network ethical mentalities; and consciously resist the dissemination of harmful information.

Network Providers also must take specific measures to protect users' Personal Information (Article 22 of the Cybersecurity Law), including to:

- Avoid installing malware on their systems;
- Immediately take remedial measures upon discovering any risk to their network products or services (such as a security defect or other vulnerability), inform users in a timely manner, and report it to the competent department; and
- Continuously provide security maintenance for network products and services and avoid terminating the provisions of security maintenance within the stipulated period (or the period agreed upon by the parties).

The Cybersecurity Law also imposes specific security management obligations on "electronic information release service providers" and "application software download service providers" (both undefined terms). If these providers find that a user has released or transmitted illegal information or malware, they should stop providing services, take necessary measures to handle or delete such information, prevent it from spreading, preserve any relevant records, and report the incident to the competent department (Article 48).

Additionally, any "critical network equipment" and "specialized cybersecurity products" must pass a security certification conducted by qualified institutions or meet the requirements of security detection before being sold or provided (Article 23). The CAC has identified four types of critical network equipment (routers, switches, rack-mounted services, and PLC equipment meeting certain specifications), and 11 specialized cybersecurity products, including certain firewalls and intrusion detection and intrusion prevention systems, in its June 1, 2017, *Catalogue (first batch) of Critical Network Equipment and Specialized Cybersecurity Products*.

Legal Liabilities and Governmental Powers

The CAC is the primary governmental authority responsible for supervising and enforcing the Cybersecurity Law; however, the CAC will delegate oversight to specific departments.

In the event of a breach of the Cybersecurity Law, depending on the nature of the offense and whether the offender is a Network Operator, CII Operator, or Network Provider, the relevant authority may:

- Order the offender to take corrective action;
- Issue a warning;
- Confiscate any illegal gains;
- Impose a fine ranging from RMB 10,000 to 1,000,000 (~$1,500 to $150,000 USD) or up to 10 times the illegal gains;
- Order the offender to suspend relevant business operations, cease business operations for rectification, or close down relevant websites;

- Revoke the offender's business permit or relevant licenses; and/or
- Impose fines ranging from RMB 5,000 to 500,000 (~$750 to $75,000 USD) or even imprison responsible management personnel.

In addition to these penalties, Article 58 of the Cybersecurity Law gives competent departments broad authority to implement "restrictions and other temporary measures against network communications in specific regions … for the purposes of maintaining national security and social public order, and handling major social security incidents…." Although the Cybersecurity Law does not specify what restrictions and measures the government can take, Article 58 is broad and could, for example, include temporarily restricting internet communication in an area, or even assuming control over the network operation of certain entities.

Indeed, authorities in China have already begun penalizing companies for noncompliance. The Public Security Bureau ("PSB"), for example, issued a warning against a technology-development company for failing to retain web logs relating to user logins in connection with its provision of internet-data services, and directing it to rectify the issue within 15 days. The PSB also has issued an order to correct an (unpublished) violation of the Cybersecurity Law against an information technology company. Companies can expect more—and likely stiffer—penalties in the future.

Extraterritorial Reach

The Cybersecurity Law has broad reach to affect even entities overseas. Specifically, Article 75 of the Cybersecurity Law makes it an offense for anyone outside of China to cause serious consequences by attacking, intruding, disturbing, destroying, or otherwise causing damage to the CII of China. In the case of a breach of this provision, in addition to other penalties under the Cybersecurity Law, the provision gives the Chinese government the authority to freeze the property of or take any other necessary sanction measures against the offender.

CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION AND IMPORTANT DATA

Perhaps the most controversial provision of the Cybersecurity Law is Article 37, the data localization requirement, which requires CII Operators to store within mainland China "citizens [P]ersonal [I]nformation and important data" collected or generated in China.

To provide guidance on this controversial data localization requirement, the Chinese government has issued draft measures and guidelines for public comment to clarify the term "important data," give guidance to businesses in China on how to protect and treat "important data," and further detail the restrictions on cross-border transfers. Specifically, on April 11, 2017, the CAC released the *Draft Measures for Security Assessment of Cross-Border Transfers of Personal Information and Important Data* ("Draft Measures").[1]

The National Information Security Standardization Technical Committee subsequently released a draft of the *Information Security Technology—Guidelines for Cross-Border Data Transfer Security Assessment* ("Draft Guidelines") on May 27, 2017. Both the Draft Measures and Draft Guidelines provide further insight into how companies can expect the Chinese government to regulate cross-border data transfers.

If issued as written, the Draft Measures and Draft Guidelines will affect nearly any foreign access to Personal Information and important data. While under the Cybersecurity Law, the data localization requirement applies only to CII Operators, the restrictions on cross-border transfer of Personal Information and important data under the Draft Measures apply to all Network Operators. Even uploading data to clouds accessible to overseas institutions, organizations, or individuals would require Network Operators to undergo security reviews and obtain privacy consents from data subjects prior to transferring Personal Information outside of China.

The following provides an overview of what information could be regarded as "important data" and the steps Network Operators need to take to lawfully transfer such "important data" and Personal Information overseas.

"Important Data" Defined

The Draft Measures define "important data" as "data closely related to national security, economic development, and social and public interest" (Article 17) (hereinafter "Important Data"). While the Draft Measures lack any further detail on this definition, the Draft Guidelines provide detailed descriptions and examples that serve to reinforce the initial concern that the term will be broadly interpreted.

First, Annex A of the Draft Guidelines indicates that data may be Important Data if its unlawful disclosure, loss, tampering, or unauthorized destruction may result in the following consequences:

- Endangering national security or national defense interests;
- Destroying international relations;
- Impairing state property, public interest, or personal legal interests;
- Impairing the state in its efforts to prevent economic and military espionage, political infiltration, and other organized crimes;
- Interfering with government departments conducting administrative activities, including supervision, management, inspection, and audit;
- Hindering government departments from performing their duties;
- Endangering the security of CII or government information systems;
- Affecting or endangering state economic order or financial security;
- Causing the release of state secrets or sensitive information; and
- Affecting or endangering the national political system, territory, military, economy, culture, society, science and technology, information, ecology, resources, nuclear facility, and other national security matters.

The Draft Guidelines further set out the scope of Important Data for 28 specific industries (fields), as well as the specified competent and supervisory authorities (if any) in charge, as summarized in Appendix A to this *White Paper*.

For those industries and specific data not listed, the Draft Guidelines set out very broad guidelines on the type of data that should be treated as Important Data, including:

- Data reflecting an industry that is closely related to national security or public interests as a whole in China;
- Data reflecting any entity as a whole that may cause a systematic risk in an industry, and data whose destruction of its integrity, confidentiality, or availability can greatly affect the steady operation of those entities;
- Data reflecting unchanging or permanently natural, economic, or social features, such as geographical positions, geomorphic features, mining locations, and genetic variation;
- Data playing a role in identifying, associating, and aggregating various data, such as geographic positions, ID numbers, mobile phone numbers, and legal person numbers (e.g., business license or other entity identifying numbers);
- Data identified by the competent authority of each industry when making important plans or decisions;
- Information that, in isolation, does not affect national security or public interests, but since it covers a large scope or long duration of time, in the aggregate may endanger or affect national security or public interests once transferred cross-border;
- Information that, in isolation, does not affect national security or public interests, but since it involves important areas or periods, in the aggregate may endanger or affect national security or public interests once transferred cross-border;
- Attribute information, vulnerability information, etc. on system designs, security protection plans, and strategy schemes of CII systems, as well as information on their units, plants, equipment, systems or plans, design capacity, and defects that are related to national security, including code technologies; and
- Information on cultural security, such as ideology and public sentiment.

The Draft Guidelines also direct the competent authorities in charge of the industries to clarify the definitions and scope, and to timely update or substitute relevant contents in the Draft Guidelines, when necessary.

Requirements for Cross-Border Transfers of Personal Information and Important Data

Both the Draft Measures and Draft Guidelines impose on all Network Operators restrictions on the transfer of Important Data and Personal Data outside of China unless certain requirements are first met.

Obtain Data Subject's Consent. Before transferring Personal Information overseas, the Draft Measures require Network Operators to notify data subjects of the purpose, scope, type, and location of the recipient, and further obtain the data subjects' consent to the transfer, except in urgent circumstances under which the security of citizens' lives and properties are endangered (Article 4 of the Draft Measures).[2]

Conduct a Security Self-Assessment. In addition to obtaining consent, before transferring Important Data and Personal Information abroad, Network Operators must develop a "Cross-Border Data Transfer Plan" and conduct a security self-assessment according to the types, amount, and importance of the data to be transferred (Articles 7-8 of the Draft Measures; Article 4.2 of the Draft Guidelines).

The Cross-Border Data Transfer Plan should include, *inter alia*, the following information:

- Purpose, scope, type, and scale of data to be transferred;
- Information system(s) involved;
- Country or region of transit (if any);
- Basic information on data recipients and their countries or regions; and
- Security control measures.

The Draft Guidelines also provide other detailed rules on how a security self-assessment should be processed (Chapters IV-V of the Draft Guidelines). For example, Network Operators should develop a security self-assessment report based on the Cross-Border Data Transfer Plan and keep it for at least five years (Article 4.5 of the Draft Guidelines). If the security self-assessment report shows that under the Cross-Border Data Transfer Plan, the transfer does not meet lawful requirements and is for valid reasons or does not meet the risk controllability requirement, Network Operators may revise the Cross-Border Data Transfer Plan, or take measures to lower the cross-border risks, and conduct a self-assessment again (Article 4.6 of the Draft Guidelines).

The lawful requirements for data transfer include that: (i) the transfer is not prohibited by laws, regulations, and official orders; (ii) the transfer conforms to treaties or agreements of data cross-border transfer that have been entered into between China and other countries or regions; (iii) consent has been obtained from the data subject, with the exception of emergencies endangering the life and property security of citizens; and (iv) the transfer excludes data identified as not prohibited for cross-border transfer by the CAC, the public security department, etc. according to law.

Valid reasons for data transfers include when such transfers are necessary to: (i) conduct regular operational activities within the legitimate scope of business; (ii) perform contractual obligations; (iii) perform legal obligations under Chinese law(s); (iv) obtain judicial assistance; and (v) safeguard the cyberspace sovereignty, national security, and public interests or protect lawful rights and interests of citizens.

Measures that may lower security risks associated with cross-border data transfers include:

- Simplifying the contents of data transferred;
- Taking technical measures to process the data within China to lower the sensitivity;
- Improving the security assurance capacity of data senders;
- Restricting the processing activities of data recipients; and
- Replacing a recipient with one that can provide higher data protections or a data recipient from an area with a greater capability to protect data based on its political and legal environment.

Additionally, in cases where the purpose, scope, type, and amount of the data to be transferred significantly varies, the data recipient changes, or the data recipient or cross-border data transfer suffers a material security incident, the Network Operator should promptly conduct another round of security self-assessments (Article 12 of the Draft Measures; Article 4.2 of the Draft Guidelines).

When Government Security Assessments are Required

According to Article 9 of the Draft Measures, the industry regulator or supervisory department must conduct the security assessment on behalf of the Network Operator if the outbound data transfer:

- Includes the Personal Information of more than 500,000 citizens;
- Entails network security information regarding nuclear facilities, chemical biology, national defense or the military, public health, large-scale engineering projects, marine environment, and sensitive geographic information;
- Involves the provision of Personal Information or Important Data to overseas recipients by CII Operators; or
- May otherwise affect national security, social, and public interests, and the competent industry regulators or supervisory authorities require review.

These criteria represent a relatively low threshold for triggering government review, and based on public comment, it is anticipated that some of these criteria will be removed or amended in the final version of the Draft Measures.

According to Article 8 of the Draft Measures, companies can expect both the security self-assessments and government-conducted security assessments to focus on the following factors:

- Necessity of the transfer;
- Amount, scope, type, and sensitivity of the Personal Information to be transferred;
- Amount, scope, and type of the Important Data to be transferred;
- Security measures and capabilities of the data recipient, and environment of data protection in the destination country or region;
- Risks arising from the data being leaked, damaged, tampered with, or misused after the transfer and subsequent retransfer; and
- Risks posed to national security, social and public interests, and individual lawful rights and interests arising from the transfer.

The relevant government authorities must provide timely feedback to Network Operators, although the detailed procedural steps have not been provided. The successful completion of the security assessment is anticipated to amount to an approval of the cross-border data transfer.

Tiered System of Protection System

The Cybersecurity Law requires the state to adopt rules for a tiered system of cybersecurity protections (Article 21). These rules likely will affect both the level of supervision and oversight the government will place on Network Operators and the security assessment process. The Cybersecurity Law does not define the term "tiered system of cybersecurity." The *Information Security Technology Classification Guide for Classified Protection of Information System*, which was promulgated and came into effect on November 1, 2008, gives some insight into what may be considered a "tiered system of protection" and provides that security protection of information systems may be divided into five tiers based on the impact of destruction of the system:

Tier I: Destruction would cause damage to the legitimate rights and interests of citizens, legal persons, and other organizations, but would cause no damage to national security, public interest, or social order.

Tier II: Destruction would cause material damage to the legitimate rights and interests of citizens, legal persons, and other organizations or cause damage to social order and public interests, but would not damage national security.

Tier III: Destruction would cause material damage to social order and public interests or would cause damage to national security.

Tier IV: Destruction would cause particularly material damage to social order and public interests or would cause material damage to national security.

Tier V: Destruction would cause particularly material damage to national security.

It remains unclear whether the Cybersecurity Law will continue to apply the current tiered protection system or will simply require additional cybersecurity protections when a system involves CII.

Prohibited Exports

According to the Draft Measures, data transfers are prohibited in any of the following circumstances:

- Where the transfer will violate laws, regulations, department rules;
- Where the data subject has not consented;
- Where the transfer may damage public or national interest;
- Where the data transfer will endanger the security of national politics, territory, military, economy, culture, society, technology, information, ecological environment, resources, or nuclear facilities; and
- Other circumstances in which the CAC, public security departments, national security departments, or other relevant departments determine that the data concerned is prohibited from being transferred overseas.

Grace Period

It is anticipated, based on the Draft Measures, that there will be a grace period for companies to comply with the rules

relating to cross-border transfer, and enforcement would start after December 31, 2018.

CYBERSECURITY LAW IN PRACTICE—RULES RELATING TO MEDICAL DEVICES

As noted, the Cybersecurity Law requires relevant industry organizations and departments to establish and improve cybersecurity protection regulations. The following section illustrates how the health care sector has responded to the Cybersecurity Law to further protect medical devices from cyberattack and similar threats.

Guiding Principles 2018

The China Food and Drug Administration ("CFDA") was the first—and thus far only—authority to have issued any formal guidance following the promulgation of the Cybersecurity Law. The CFDA issued the *Guiding Principles on the Technical Reviews of the Cybersecurity Registration of Medical Devices* ("Guiding Principles") on January 20, 2017, which will take effect on January 1, 2018.[3]

The Guiding Principles apply to the registration of Type II and Type III medical devices that can be controlled remotely or connected to networks in order to conduct electronic data exchanges, as well as to Type II and Type III medical devices that use storage media to conduct data exchanges. Like other guiding principles issued by the CFDA, the Guiding Principles are not mandatory. When registering medical device products, an applicant may conduct a self-assessment on whether certain measures proposed under the Guiding Principles should apply. If the applicant decides that any measures proposed under the Guiding Principles should not apply, it may elaborate the reasons and/or propose alternative solutions to ensure its compliance with the Cybersecurity Law and other relevant regulations, measures, and guidelines.

According to the Guiding Principles, the cybersecurity protections of medical devices include the confidentiality, integrity, availability, authenticity, accountability, nonrepudiation, and reliability of the data generated and used by medical devices. Beyond the registration stage, an applicant for a medical device registration should continuously be aware of cybersecurity issues involved in the design, development, manufacture, distribution, and maintenance throughout the entire life cycle of a medical device.

An applicant should include the following information in its registration application materials in the section on "Software Research, Product Technical Requirements, and Product Instructions":

- Data transfer protocol;
- Data storage format used; and
- User access-control mechanisms (e.g., user authentication, type of user, and user authorization).

An applicant also should include a stand-alone cybersecurity description file and a cybersecurity instruction manual, which details:

- The type of data (personal data of users or device operations data);
- The function of the medical device;
- The function of the medical device software (one-way or two-way data exchange, real-time, or non-real-time remote control, etc.);
- Data exchange methods and requirements, data storage formats, requirements, and capacity, together with proof of satisfying radio management regulatory requirements;
- Information on security software, such as antivirus software or firewall; and
- Information on preinstalled software.

An analysis report of cybersecurity risk management, relevant test plans, and reports, and a maintenance plan, also should be included.

When there is a major cybersecurity update affecting the safety or effectiveness of the medical device after the initial registration, the applicant is required to submit a stand-alone cybersecurity description file, with the information as described above, to amend its application. When there is a minor cybersecurity update not affecting the safety or effectiveness of the medical device after the initial registration, an immediate amendment application is not required. An

applicant only has to submit a security patch file when it is required to make a registration application again. A security patch file should include the description of the update, the test plans and reports, and proof that any new known risks are acceptable. When an applicant is required to reregister the medical device and there is no cybersecurity update, an authenticity statement is required.

When reviewing registration of medical devices covered by the Guiding Principles, the CFDA will consider: (i) the type of data (personal data of users or device operations data); (ii) technologies used in the medical devices; and (iii) the potential impact of preinstalled software in the medical devices.

With regard to the type of data, the CFDA will consider, *inter alia*, the network interface, network bandwidth, data transfer protocol, real-time control, and data storage format used. An applicant is required to satisfy all the applicable regulatory requirements concerning personal data protection. If dealing with radio equipment, an applicant is required to satisfy all the applicable regulatory requirements concerning radio management.

With regard to the technologies used, considerations include user access-control mechanisms (e.g., user authentication, user authorization, password strength, and software update authorization), data encryption mechanisms (e.g., verification, e-signature, and standard protocol), and attack prevention and response mechanisms (e.g., firewalls, intrusion detection, and a mitigation and recovery plan). Applicants may refer to the relevant national and international standards such as IEC/TR 80001-2-2 and technical reports to establish their cybersecurity capabilities.

With regard to any preinstalled software, an applicant is required to demonstrate that it is able to monitor the preinstalled software, provide necessary updates and patches in time, and keep accurate logs.

Implications

Network Operators in other industries can see from the Guiding Principles that China intends to apply the Cybersecurity Law practically. Instead of creating a new regulatory system specifically to implement the Cybersecurity Law, which can be both expensive and time-consuming, the CFDA has chosen to incorporate the requirements under the Cybersecurity Law into the existing review system by adding additional criteria for the registration of medical device products. It is likely that other regulatory or competent departments will use similar methods to implement the Cybersecurity Law in other industries. Mandatory or not, Network Operators are strongly advised to comply with applicable requirements and guidelines.

OTHER REGULATIONS AND GUIDELINES

In addition to the Guiding Principles, Draft Measures, and Draft Guidelines discussed above, the Chinese government also issued the *Measures for the Security Assessment of Network Products and Services 2017 (for Trial Implementation)* ("Trial Measures") in May 2017, which became effective as of June 1, 2017. Under the Trial Measures, the CAC, Network Security Review Board and Network Security Review Office, and authorized third-party institutions are to assess the security of network products and services. The Trial Measures provide Network Providers the right to report to the Network Security Review Office or relevant department if they believe that certain authorized third-party institutions are not making objective and impartial assessments, or that the third-party institutions are breaking their obligation of confidentiality with regard to the information obtained during the assessment process. However, further guidance is necessary regarding how such assessments will work, or whether there are any limitations on the power of the authority itself.

SUGGESTIONS FOR FOREIGN INVESTORS

China's implementation of a new cybersecurity regime will continue to be in flux for some time. In the interim, companies can take certain steps to comply with the ever-evolving legal framework in light of what is known and anticipated for implementation of the Cybersecurity Law.

Be Prepared

Companies that are or may be subject to the Cybersecurity Law should:

- Review and assess the Personal Information and other data, including any Important Data, collected by the company (collectively, "Restricted Data");

- Identify recipients and location of recipients of Restricted Data;
- Consider whether all or part of the Restricted Data should or can be stored and processed in China. It is important to note that the list of industries and fields with specific types of Important Data that the Draft Guidelines identified (as summarized in Appendix A to this *White Paper)* is not exhaustive. Therefore, even if the industry in which a business is operating is not currently referenced, businesses should still consider carefully the impact of destruction, loss of functions, or data leakage of such data in light of the general guidance, in order to decide whether the data could be regarded as Important Data subject to restrictions;
- Assess the measures in place to protect Restricted Data and systems in light of the anticipated security assessment process and update relevant organizational, technical, and security protections;
- Identify whether the company has adequate consents from relevant data subjects and, if not, obtain or update such consents. This may involve updating standard employment and other contracts; and
- Carefully consider whether the company does or may function as a CII Operator, and thus subject to heightened obligations to protect Restricted Data.

Monitor General and Industry Regulations

In addition to those regulations identified in this *White Paper*, it is expected that the CAC and relevant industry organizations will publish further detailed and practical guidance on the Cybersecurity Law in the coming months. The timeline on when future regulations or guidelines will be published—and what further obligations they will impose—has not been released, so regular monitoring is essential. Not all regulations or guidance will provide a grace period.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Elizabeth Cole
Singapore / Shanghai
+65.6538.3939 / +86.21.2201.8024
ecole@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Jörg Hladjk
Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Chiang Ling Li
Hong Kong
+852.3189.7338
chianglingli@jonesday.com

Michael W. Vella
Shanghai
+86.21.2201.8162
mvella@jonesday.com

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Special thanks to associates Stephanie Li, Erin Shi, Jennifer Everett, Frances Forte, Kerianne Tobitsch, and Grace Zhang, who contributed to the preparation of this White Paper.

ENDNOTES

1 The deadline for submissions of public comments was May 11, 2017. Following the public comment period, on May 19, 2017, the CAC invited selected stakeholders to attend a seminar and discuss an updated version of the Draft Measures (second draft), purportedly reflecting some of the concerns supplied by international stakeholders during the public comment period. The CAC is still making further amendments prior to formal issuance of the updated Draft Measures.

2 Consent is deemed obtained when data subjects make international phone calls, send international emails, conduct international instant messaging, or conduct cross-border trading through internet and other activity.

3 The Guiding Principles are supplements to the *Guiding Principles on the Technical Reviews of the Registration of Medical Device Software*, which were issued and came into effect on August 5, 2015.

APPENDIX A

Industries (Fields)	Examples of Important Data	Competent Authorities	Supervisory Authorities
Oil and gas	Data on values, production and sales volumes, construction workloads, safety and environmental protection, and reserves.	National Development and Reform Commission; National Energy Administration	—
Coal	Data on basics, economy, purchase, production, sales, and investment.		
Petrochemical	The main economic-technical indicators for annual, medium-, and long-term development plan; the key policies and measures for the petroleum and petrochemical industry in China; annual import plan for key production materials of the petrochemical industry; controlled foreign exchange amount not appropriated.	National Energy Administration	
Power	Information on power plants; power transmission and distribution; and construction, operation, and maintenance.	National Development and Reform Commission; National Energy Administration	
Communication	Ratio data; data on planning and construction, operation and maintenance, security assurance, and statistical analysis.	Ministry of Industry and Information Technology	
Electronic information	Industrial operation data; data on industrial development; business data on top 100 electronic information enterprises; technical data; information on sales and application of electronic information equipment in key industries and sectors; information on the operation, maintenance, and servicing of electronic information products during application in key industries and sectors; information, relating to government secrets, business secrets, or individual privacy, that is collected, stored, managed, or analyzed during the application of electronic information products in key industries and sectors.		
Iron and steel	Information on the strength, potential, and competitiveness of the industry; the strength of industry of products required for national defense, military affairs, and national economic development; and national industry development, external environment control, and countermeasures.		
Non-ferrous metal			
Equipment manufacturing	Information on investment and production.		
Chemical industry	Statistical data; information on projects in important regions and the export of military chemical products; information on the transportation of violently poisonous, explosive, or dangerous chemicals; information on companies producing or storing dangerous chemicals as well as the communication, warning devices, safekeeping measures applied to the workplaces; assessment report issued by the competent agency in view of the safety requirements in production for chemical enterprises; information on construction projects that are newly constructed, reconstructed, expanded, and used to store, load, or unload dangerous chemicals; information on workshop and storehouse; information on the quantity and whereabouts of violently poisonous, explosive, and dangerous chemicals produced or stored by the enterprises.		

Industries (Fields)	Examples of Important Data	Competent Authorities	Supervisory Authorities
National defense and military industry	Information on the companies; purchased components and parts, software, and testers for industrial control equipment.	State Administration of Science, Technology, and Industry for National Defense	
Geography	Geographic information on key targets and important locations, special mapping information, open map data, Beidou satellite navigation information.	Ministry of Land and Resources of China; National Bureau of Surveying and Mapping Geographic Information, State Oceanic Administration	
Civil nuclear facilities	Information on security supervision and operation of civil nuclear facilities; industrial development of nuclear facilities.	State Administration of Science, Technology, and Industry for National Defense; National Energy Administration Security	State Nuclear Safety Bureau, Environmental Protection Department
Transportation	Data containing information on or radio spectrum deployed by communication system relating to transportation.	National Transport Combat Readiness Office, Ministry of Transport of China; National Railway Administration of China	
Post and express service	Confidential information obtained during the service.	State Post Bureau of China	