
Recent Developments in Chinese Cybersecurity and Information Technology Regulations

JUNE 3, 2019

The Chinese government has recently issued a flurry of regulations and standards, several in draft form for public comment, to implement the Cybersecurity Law. These mostly reflect a lengthy policy development process instituted after enactment of the Cybersecurity Law in 2016, and in some instances will replace less comprehensive interim documents.

The Cybersecurity Administration of China (CAC) on May 24 issued the draft Measures on Cybersecurity Review (“draft Measures”), with comments due by June 24. The draft Measures will replace the Measures for Security Review of Network Products and Services (for trial implementation, 2017). The draft Measures consist of 21 articles and apply to the operation of critical information infrastructure (CII). CII is largely defined as network facilities and information systems which, were they to fail, would seriously jeopardize public security and public welfare (e.g., public communications and information services, power, traffic, water, finance, public service, and electronic governance), which should mean that the draft Measures will not apply to most foreign-invested enterprises (FIEs) because of restrictions on foreign investment in CII. Financial services and healthcare services are among the exceptions. However, FIE providers of information technology (IT) and other vital technology to CII operators will have their business impacted by security reviews of procurement decisions by CII operators.

The draft Measures provide for establishment of a national cybersecurity review work mechanism with membership from the CAC, National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of State Security, Ministry of Commerce, Ministry of Finance, People’s Bank of China, State Administration for Market Regulation, National Radio and Television Administration, National Administration for the Protection of State Secrets, and Office of the State Commercial Cryptography Administration (OSCCA)—in other words, the country’s leading security, economic planning, industrial development, financial and broadcast regulators. A Cybersecurity Review Office (“Office”) will be housed in CAC to organize cybersecurity reviews and supervise the implementation of cybersecurity review determinations (Article 5).

CII operators are required to identify and forecast potential security risks prior to procurement of products or services, prepare security risk reports with respect thereto, and apply to the Office for a

cybersecurity review if any of the following risks are anticipated (Article 6):

- (i) complete shutdown or failure of the main functions;
- (ii) leakage, loss, corruption or cross-border transfer of large quantities of personal information (PI) or important data (ID);
- (iii) threats to supply chain security that may compromise operation or maintenance, technical support, or upgrades; or
- (iv) other catchall potential risks that may severely impair CII.

The Office will have 30 working days (extended to 45 working days in complex cases) to review the reports by CII operators (Article 9). The Office will focus on potential national security risks created by the procurement activity and take into account several factors, including foreign government financial support for the product or service provider; impact on continuing secure and stable operation of the CII; potential leakage, loss, corruption or cross-border transfer of large quantities of PI or ID; and controllability, transparency and security of the supply chain for the product or service, including the possibility of interruption due to political, diplomatic, trade or other nontechnical factors (Article 10). In other words, the possibility of an embargo imposed by a foreign government would be taken into account.

CII operators may apply to the Office through their industry regulator for review by the full working mechanism of an adverse determination, with a decision to be made within 15 working days (Article 11). If the members of the working mechanism do not reach a unanimous decision within such time period, a special review may be undertaken over the next 45 working days, subject to extension if necessary. Ultimate authority to review the applications rests with CAC, which is likely to be the most influential member of the working mechanism in general (Articles 12-13). Critically, commercial contracts subject to the cybersecurity review procedure become valid only after cybersecurity review clearance (Article 7).

Providers of products and services subject to this cybersecurity review procedure will also be required in most instances to comply with three recently issued national standards that will enter into effect in December, replacing older standards that predate recent developments in technology. The three standards are:

- GB/T22239-2019 Information Security Technology (Baseline for Classified Protection of Cybersecurity) (2019 Baseline, replacing the 2008 version)
- GB/T25070-2019 Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity (replacing the 2010 version)
- GB/T28448-2019 Information Security Technology – Evaluation Requirement for Classified Protection of Cybersecurity (replacing the 2012 version)

The GB/T designation signifies that the standards are voluntary rather than compulsory GB national standards, but in practice, GB/T standards tend to be widely adopted.

The major changes embodied in these standards are the specification in GB/T22239-2019 of

general and expanded security requirements to newer technologies (cloud computing, mobile communications, IoT and industrial control systems) in accordance with the five-level Multi-Level Protection Scheme (MLPS). Technologies dependent on their security will be classified as MLPS 1, 2, 3 or 4. Level 5 is the highest level and falls outside the scope of commercial procurement under GB/T22239-2019.

Requirements include assurance that cloud service customer data and user PI are stored in China, and compliance with applicable rules for cross-border data transfer.

Levels 2, 3 and 4 cloud service producers and third parties qualify for data management only after authorization by their cloud service customers. Operational maintenance of cloud service platforms must be conducted in China, subject to exceptions that must comply with specific requirements.

Critically, procurement and use of encryption cybersecurity products and services of Levels 2, 3 and 4 must comply with OSCCA requirements. Only OSCCA-certified and verified encryption technology and products may be used for these levels. In other words, commercial encryption technology and products must first be submitted to OSCCA before they can be procured and installed for MLPS 2, 3 or 4 uses.

Additionally, cloud computing infrastructure must be located in China.

Authors



Lester Ross

PARTNER

✉ lester.ross@wilmerhale.com

☎ +1 202 663 6000