OVERVIEW OF THE NEW IMPLEMENTING RULES ON CRITICAL INFORMATION INFRASTRUCTURE IN CHINA AND KEY TAKEAWAYS

Date: 19 October 2021

China Data Protection, Privacy, and Security Alert

By: Amigo L. Xie, Xiaotong Wang, Yibo Wu, Prudence Pang

On 30 July 2021, the State Council promulgated the Regulations on the Security Protection of Critical Information Infrastructure (the Regulation), which took effect on 1 September 2021. This Regulation dovetails with the upper-level legislation of the PRC Cybersecurity Law (effective on 1 June 2017), further delineating the scope and security obligations of the operators of "critical information infrastructure" (the CII), for purposes of cybersecurity and data security in China.

When the PRC Cybersecurity Law was enacted in November 2016, it broadly defined CII the first time. However, the State Council was left to clarify the specific scope and security obligations of CII operators. As CII operators are required to locally store the personal information and important data they collected in China and the transfer of such information and data is subject to a government-performed national security review, it is imperative for companies and individuals to understand if their operations fall within the scope of CII or CII operators. In 2017, the State Council prepared a draft regulation (2017 Draft), which was subsequently finalized into this Regulation.

This alert highlights important provisions and key terms within the Regulation, including the authorities-in-charge, the identification mechanism of CII, and the primary security obligations of a CII operator. It concludes with key takeaways, which outline the likely impact of the Regulation on multinational companies that are conducting business in or with China.

I. THE AUTHORITIES-IN-CHARGE AND SECURITY PROTECTION DEPARTMENTS

The relevant authorities in charge under the Regulation include:

- **Cyberspace Administration of China (CAC)**: responsible for the overall coordination.
- **Ministry of Public Security**: responsible for guiding and supervising the security protection of CII.
- **Ministry of Industry and Information Technology**: responsible for the security protection, supervision and administration of CII, along with other relevant ministries of the State Council, in their respective areas.

The provincial-level delegates of the above authorities in charge are also responsible for the protection and administration of CII according to their respective duties in the relevant Chinese provinces.

More importantly, the competent departments and regulatory departments governing key industries and areas are specifically and directly responsible of the security protection of CII (the Security Protection Departments), including identification of a CII operator under the Regulation.

II. SCOPE OF CII

The CII under the Regulation is defined from two perspectives:

- The industries test: the "important network facilities and information systems" (the Facilities & Systems) in the following industries and fields: (i) public telecommunication and information service, (ii) energy, (iii) transport, (iv) water conservancy, (v) finance, (vi) public service, (vii) e-government, (viii) science and technology industry for national defense, and (ix) other important industries and fields; or
- The consequences test: other Facilities & Systems which may seriously endanger the national security, national economy, people's livelihood and public welfare once they are subject to any destruction, loss of function or data leakage.

The above scope of CII covered in the Regulation is largely the same as that under the PRC Cybersecurity Law and inherits the "catch-all" description. However, it explicitly adds the item (viii) science and technology industry for national defense, as noted in the industries test.

III. IDENTIFICATION MECHANISM

In principle, the Regulation indicates that an operator is a CII operator when and if the relevant Security Protection Departments so decide and notify such operator. This shifts the burden of proof to the Security Protection Departments to some extent and provides a kind of certainty to market players. The Regulation adopts a three-step mechanism to identify CII:

1. **Rulemaking**: the Security Protection Departments will formulate the rules for identification of CII according to the actual conditions of the respective industries and areas (Identification Rules), and submit such Identification Rules to the Public Security Department under the State Council for record-filing.
2. **Identification**: the Security Protection Departments are responsible for organizing the identification of CII in their respective industries and areas in accordance with Identification Rules and should in a timely manner notify a CII operator of the identification results and report the identification results to the Public Security Department under the State Council.
3. **Report of Major Changes**: a CII operator shall in a timely manner report to the relevant Security Protection Department any major changes to the CII which may affect the identification result, the Security Protection Department shall re-conduct the identification within three months upon receiving the report from the CII operator.

IV. KEY OBLIGATIONS OF CII OPERATORS

Under the Regulation, the primary security obligations of a CII operator include:

- planning, constructing, and utilizing the security protection measures/facilities simultaneously with CII;

- appointing a principal to take the lead in the security protection of CII, handle major cybersecurity incidents, and organize the analysis and settlement of major cybersecurity issues;
- setting up and providing enough operational funds to an internal specialized security management committee to enable the committee to conduct protection duties and make relevant decisions;
- conducting annual cybersecurity detection and risk assessment of CII, timely rectifying any security problems identified, and reporting any issues, as required, to the Security Protection Departments;
- giving priority to safe and trusted providers of online product and services, signing security and confidentiality agreements with online product and service providers in the procurement process, and reporting for national security review if such procurement may affect national security interests; and
- reporting any of its merger and acquisition deals to the Security Protection Departments and taking protective measures for the CII as required.

If in breach of a key obligation, a CII operator may be subject to a fine from RMB 100,000 to 1 million if it refuses to make corrections or it endangers cybersecurity or causes other consequences. A fine of RMB 10,000 to 100,000 may be imposed on the directly responsible officer in charge.

Where a CII operator fails to conduct a national security review during the procurement of online products or services that may affect national security, it will face a fine of one to 10 times of its procurement price, and a fine of RMB 10,000 to 100,000 may be imposed on the officer directly in charge and other directly liable persons.

V. INFLUENCE ON MULTINATIONAL CORPORATIONS (MNCS) AND KEY TAKEAWAYS

4. **Scope/Identification of CII**. This Regulation provides a clearer identification mechanism and imposes an obligation of the Security Protection Departments to notify the CII operators they have identified based on the Identification Rules. The Regulation's implementation will have to be tested and tracked closely. Generally speaking, CII cannot be classified solely based on entities but needs to be assessed comprehensively and dynamically together with the importance of the business, the critical business information flows, amongst a variety of other considerations.
5. **MNCs acting as a CII operator in China**. When a subsidiary of an MNC in China receives a CII identification notice from the relevant Security Protection Department, it should comply with the Regulation and discharge its key obligations mentioned above.
6. **MNCs supplying products or services to a CII operator in China**. If an MNC is a supplier of products or services to a CII operator in China, it should anticipate that more extensive due diligence may be conducted by the CII operator, and that the arrangement will be subject to additional confidentiality obligations, or even a national security review. In light of this, MNCs doing business in or with China-based businesses should consider enhancing their network security protection and have internal rules and necessary facilities to avoid being disqualified as a supplier to CII operators due to non-compliance or security concerns.

There will be many additional important developments as the Security Protection Departments formulate the Identification Rules and, ultimately, implement the Regulations. Should you have any questions or concerns about the Regulations or other legal developments in China, reach out to our China-based lawyers.

KEY CONTACTS

AMIGO L. XIE
PARTNER

HONG KONG
+852.2230.3510
AMIGO.XIE@KLGATES.COM

XIAOTONG WANG
ASSOCIATE

BEIJING
+86.10.5817.6119
XIAOTONG.WANG@KLGATES.COM

YIBO WU
ASSOCIATE

SHANGHAI
+86.21.2211.2090
YIBO.WU@KLGATES.COM

PRUDENCE PANG
ASSOCIATE

HONG KONG
+852.2230.3519
PRUDENCE.PANG@KLGATES.COM

