COVINGTON

China Seeks Public Comments on Draft Regulation on the Protection of Critical Information Infrastructure

July 12, 2017

Data Privacy and Cybersecurity

On July 11, 2017, the Cyberspace Administration of China (CAC) released the draft *Regulation for the Protection of the Critical Information Infrastructure ("Draft Regulation")* for public comment (official Chinese version available here). The comment period ends on August 10, 2017.

Aiming to add greater clarification to the Cybersecurity Law, which took effect on June 1, 2017, the Draft Regulation clarifies the scope of Critical Information Infrastructure ("CII") and elaborates on how CII operators are supposed to protect their networks against cyber threats. The Draft Regulation also sets out additional obligations CII operators face, including allowing officials to perform cybersecurity inspections, among others.

The Draft Regulation may help reduce some of the confusion surrounding the key phrase "critical information infrastructure," which constitutes a crucial part of China's fast-evolving cybersecurity regulatory framework. But many important questions remain unanswered in the current draft. Companies that either operate in the sectors identified in the Draft Regulation or that supply operators in those sectors should be mindful of the requirements relating to cybersecurity, especially relating to cybersecurity reviews and procurement of network services and products, and closely monitor the regulatory developments.

Key elements of the Draft Regulation are summarized below.

Classification of CII and CII Operators

The Cybersecurity Law defines CII broadly as "infrastructure that, in the event of damage, loss of function, or data leak, might seriously endanger national security, national welfare or the livelihoods of the people, or the public interest." Article 31 of the Cybersecurity Law references a number of "key sectors," including telecommunications, energy, transportation, water conservation, financial services, utility, and e-government.

Article 18 of the Draft Regulation further clarifies the scope of CII, specifying that "critical network infrastructure and information systems" operated or managed by entities in the sectors identified below should be considered CII, if such infrastructure, "in the event of damage, loss of function, or data leak," may "seriously endanger national security, national welfare or the livelihoods of the people, or the public interest." The entities that can be identified as operators of CII include:

- Governmental agencies, and entities in the sectors of energy, finance, transportation, water conservation, healthcare, education, social insurance, environmental protection, utilities and so on;
- Information network operators such as operators of telecommunication, broadcasting networks, and the Internet, as well as service providers of cloud computing, big data, and other large-scale public information services;
- "Manufacturing and research and development entities" in sectors such as national defense, large-scale equipment, chemical engineering, and food and drugs;
- "News units," including broadcasting stations, TV stations, and news agencies; and
- "Other key sectors."

Although the Draft Regulation identified more sectors within which key infrastructure may be considered CII, whether a particular company operating in one of those sectors will be deemed as a CII operator remains unclear. The Draft Regulation states that to provide more guidance for sector regulators (which are tasked with identifying CII in their respective sectors), the CAC, Ministry of Industry and Information Technology ("MIIT"), and Ministry of Public Security ("MPS") are working together to draft the *Guidelines on the Classification of Critical Information Infrastructure*. Sector regulators will be required to identify and report CII operators in their respective sector to the CAC according to procedures that are forthcoming in those guidelines.

Cybersecurity Requirements for CII Operators

If a company is identified as a CII operator, it will be subject to a number of requirements identified in Articles 21 to 29 of the Draft Regulation. These requirements are largely consistent with the corresponding provisions in the Cybersecurity Law.

- *Cybersecurity Governance and Leadership*
  - The Draft Regulation requires that the primary responsibility of protecting CII shall be shouldered by the operator's senior leadership (Article 22). The senior leadership must be in charge of ensuring cybersecurity across the organization and implementing a comprehensive cybersecurity program.
  - Furthermore, CII operators are required to appoint a dedicated cybersecurity organization and a manager responsible for cybersecurity (Article 24.1). The operators must conduct background checks on these dedicated cybersecurity managers. The cybersecurity manager position, which is somewhat akin to a Chief Information Security Officer position, is responsible for the following (Article 25):
    - Setting the organization's cybersecurity policies and procedures;
    - Assessing the skills of personnel in critical cybersecurity positions;
    - Establishing and implementing a cybersecurity education and training plan;
    - Performing cybersecurity examinations and incident response exercises; and
    - Reporting important cybersecurity incidents to relevant national authorities as required by law.
  - CII operator personnel in critical cybersecurity positions must be certified by the relevant regulators (Article 26).

- CII operators will be expected to organize annual training and education sessions for cybersecurity personnel for no less than one day per year. For personnel in critical cybersecurity positions, there must be no fewer than three days of training per year. (Article 27)

- *Cybersecurity Measures*
  - Article 21 of the Cybersecurity Law requires network operators to "safeguard networks against disruption, damage or unauthorized access, and prevent data leakage, theft, or tampering." The Draft Regulation holds CII operators to the same requirements, but provides more detail on what is expected. The steps that CII operators must take to protect CII include (Article 23):
    - Establishing internal cybersecurity management program and protocols, and strictly following access control policies (to limit the access to authorized users and authorized activities);
    - Utilizing the technical measures required to defend against cybersecurity threats such as computer viruses, network attacks, and network intrusion;
    - Utilizing the technical measures required to monitor network security status, log security incidents, and store the relevant network logs for at least six months; and
    - Utilizing data encryption and classification measures as necessary.
  - Moreover, Article 24 of the Draft Regulation largely reiterates cybersecurity obligations set by Article 34 of the Cybersecurity Law for CII operators, and provides that CII operators must follow the mandatory requirements in relevant national standards and take the following steps:
    - Appoint a dedicated cybersecurity organization and a manager responsible for cybersecurity, and conduct a background check on the manager;
    - Conduct cybersecurity education and technical trainings and assess the skills of cybersecurity personnel on a regular basis;
    - Maintain a disaster recovery backup for important systems and databases, and take measures to address security risks (such as system vulnerabilities) in a timely fashion;
    - Formulate incident response plans for cybersecurity incidents and organize testing on a regular basis; and
    - Address other obligations prescribed by laws and administrative regulations.
  - Article 21 requires that cybersecurity measures be planned, constructed, and used during construction of CII, a requirement that may be seen as similar to "security by design" principles in other jurisdictions.

- *Annual Security Assessment*
  - Consistent with Article 38 of the Cybersecurity Law, Article 28 of the Draft Regulation requires CII operators to establish a comprehensive security assessment process and conduct security assessment when new CII starts operating or is going through major changes. CII operators should also conduct annual security assessment and report the result of such assessment to sector regulators.

Data Localization and Cross-Border Transfers

The Draft Regulation references– but does not provide additional detail on– requirements for data localization and cross-border data transfers. In accordance with Article 37 of the Cybersecurity Law, Article 29 provides that data collected or generated in the course of operations within the People's Republic of China must be stored locally. Where it is necessary to transfer such data abroad by CII operators, a security assessment must be carried out based on the *Measures on Security Assessment of Cross-Border Data Transfer of Personal Information and Important Data*.

Security of Products and Services Used

The Draft Regulation devotes a chapter to the supply chain security requirements that CII operators are expected to meet for network products and services they use in their operations. Articles 30 through 34 reiterate the requirements imposed by the Cybersecurity Law and introduce a few new requirements:

- Ensure that Critical Network Equipment and Network Security Products procured by CII operators must be in compliance with the mandatory requirements of relevant national standards (related to Article 23 of the Cybersecurity Law);
- Ensure that procurement of "network products and services" that may implicate China's national security will go through the cybersecurity review, and the CII operators must sign security and confidentiality agreements with the suppliers (related to Articles 35 and 36 of the Cybersecurity Law);
- Conduct a security assessment before using systems and software developed by outsourced third parties and network products donated by external parties;
- Take steps to eliminate cybersecurity vulnerabilities of network products and services that CII operators are using and report serious risks to the relevant agencies; and
- Carry out the operation and maintenance of CII within China; if it is necessary for the maintenance of CII to be performed outside of China, CII operators must report this to the sector regulators and MPS beforehand.

Article 35 also anticipates more guidelines to be issued by CAC and other regulators with respect to conducting a security assessment for CII operators, publishing cybersecurity threat information, and providing cloud and other outsourced services to CII operators. CII operators and their suppliers should follow these guidelines as they are released.

Cybersecurity Threat Monitoring, Incident Response, and Cybersecurity Inspections

In addition to the internal cybersecurity measures discussed above, the Draft Regulation provides more guidance on how CII operators should interact with agencies on cybersecurity issues, including information sharing, threat monitoring, and cybersecurity inspections.

- Information sharing: reiterating Article 39 of the Cybersecurity Law, the Draft Regulation provides that CII operators are expected to partake in the cybersecurity information sharing scheme coordinated by CAC (Article 38).
- Threat monitoring: the Draft Regulation provides that the CAC, with the participation of sector regulators, will establish an early threat monitoring system and a notification system that will disseminate threat information to CII operators (Articles 36 and 37).

- Cybersecurity inspections: notably, the Draft Regulation requires CII operators to undergo a cybersecurity inspection, which includes allowing sector regulators to access, retrieve, and reproduce relevant documents or records and conduct technical assessment for the protective measures (Articles 40 to 42).

Penalty for non-compliance

- *Penalties for Failing to Comply with Cybersecurity Protection Obligations*: CII operators who fail to comply with their cybersecurity obligations will be issued a warning and may face fines between 100,000 and 1,000,000 RMB (Article 45).
- *Penalties for Violating Data Localization Requirements:* CII operators who violate data localization requirements may have any illegal gains confiscated, may face fines between 10,000 and 100,000 RMB, and may be ordered to cease business operations (Article 46).
- *Penalties for Using Unapproved/Insecure Products or Services*: CII operators who are found to have violated Article 31 may be ordered to cease the use and face fines between 10,000 and 100,000 RMB (Article 47).
- *Sanctions for Foreign Entities*: Foreign entities discovered to have engaged in cyberattacks, intrusion, hacking, or interference with China's CII could face "necessary sanctions," including, for example, asset freezes (Article 52).

Potential Implications

Companies active in China should continue to follow these legislative developments and be watchful for future guidelines that explain how to determine whether a company operating in the enumerated sectors discussed above will be deemed as a CII operator. Moreover, companies that supply network products and services to entities in key sectors should be aware of how the Draft Regulation may affect their sales and post-sale activities in China, if their customers are deemed to be CII operators.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
Jenny Martin	+1 650 632 4737	jrmartin@cov.com
Ted Karch	+1 415 591 7094	tkarch@cov.com