Updates
October 25, 2021

China Releases New Regulations on the Protection of Critical Information Infrastructure

On August 17, 2021, China released the new regulations on the Security and Protection of Critical Information Infrastructure (CII Regulations), which became effective on September 1, 2021. Even though China started its protection of Critical Information Infrastructure (CII) as early as 2016, when it released the Cybersecurity Law of the People's Republic of China (CSL), there is no clear guidance on the identification of CII and its operators. The new CII Regulations provide general guidance on formulating CII identification rules by competent regulatory authorities in relevant important sectors. In addition, the CII Regulations provide more specific rules on the protection of CII to implement the requirements in the CSL. This update discusses the highlights of the CII Regulations.

Definition and Identification of CII

Under the CII Regulations, critical information infrastructure refers to important network facilities and information systems in important sectors, such as public communication and information services, energy, transportation, water conservation, finance, public services, e-government affairs, and science and technology industries for national defense, as well as other important network facilities and information systems that may endanger national security, national welfare, people's livelihoods, and the public interest in case of damage, loss of function, or data breach. (Art. 2) Abandoning a more specific approach of listing relevant businesses in important sectors in the draft CII Regulations released in 2017, the official CII Regulations adopt a broader definition similar to that in the CSL.

The CII Regulations further require the competent as well as regulatory and administrative departments in the above-mentioned important sectors (Protection Departments) to formulate CII identification rules based on the actual situations of their respective sectors and submit such identification rules to the Ministry of Public Security (MPS) for recordal. Such Protection Departments shall take into account the following factors when making the CII identification rules:

- Importance of the network facilities and information systems to the critical and core business of their respective sectors.
- The harm that might be caused in case of damage, loss of function, and data breach of the network facilities and information systems.
- Relevance and impact on other sectors. (Art. 9)

The CII Regulations further provide that the Protection Departments shall be responsible for identifying the CII in their respective sectors according to the CII identification rules and notifying relevant operators promptly. CII operators will need to report any significant changes to the CII that might affect the result of identification to the Protection Departments. The Protection Departments shall complete the re-identification within three months from the date of receiving such report and notify the CII operators. (Arts. 10, 11)

Companies in the above-mentioned important sectors not yet identified as CII operators should closely monitor the formulation process of the CII identification rules in their respective sectors and pay attention to any official

identification notice that might come from the Protection Departments. According to our experience, this notification approach is consistent with what the government has been doing in practice in the past few years. Companies already identified as CII operators should pay attention to the requirement of reporting significant changes (e.g., building new machine rooms or systems) to the Protection Departments as mentioned above.

Authorities to Be Responsible for Protecting Personal Information

Under the CII Regulations, the Ministry of Public Security (MPS) will be responsible for the guidance and supervision of CII protection, with overall coordination handled by the Cyberspace Administration of China (CAC). The Ministry of Industry and Information Technology and other relevant authorities under the State Council as well as relevant authorities of the local government at the provincial level will also be responsible for CII protection and supervision and management within their respective scope of duties. (Art. 3) In addition, the Protection Departments, as mentioned above, will be responsible for the CII protection in their respective sectors. (Art. 8)

Compared with the draft CII Regulations, the official CII Regulations emphasize the role of the MPS in CII protection and move the level of the local government responsible for CII protection and supervision and management from the county level to the provincial level.

Obligations of Operators of the Critical Information Infrastructure

According to the CII Regulations, the CII operators will need to establish and improve their cybersecurity protection and accountability systems. The CII Regulations require the operators to take protection measures at the stages of CII planning, construction, and use. The main responsible person at each operator will have overall responsibility for CII protection and take the lead in CII protection and handling of major cybersecurity incidents. (Arts. 12, 13)

Also, the CII Regulations require the operators to set up a specialized security management team and conduct background checks on the responsible person and the personnel in key positions on such team. (Art. 14) The specialized security management team will be responsible for the following work related to the CII protection of the operator:

- Establishing and improving the operator's cybersecurity management and performance evaluation system as well as drafting a CII protection plan.
- Building cybersecurity safeguard capabilities, conducting cybersecurity monitoring, and conducting cybersecurity testing and risk assessment at least once a year.
- Formulating an emergency plan, conducting emergency drills, and handling cybersecurity incidents.
- Identifying key positions, conducting performance evaluations, and making suggestions regarding rewards and punishment.
- Conducting cybersecurity training.
- Performing data protection duties and establishing and improving data protection systems.
- Conducting security management for CII design, construction, operation, maintenance, and other services.
- Reporting major cybersecurity incidents and threats and other important matters (e.g., merger, separation, or dissolution of the CII operator) to the Protection Departments. (Art. 15)

It is noteworthy that such a specialized security management team must be involved in the decision-making process regarding cybersecurity and information technology issues. (Arts. 16, 17, 18, 21)

Companies should pay attention to the above-mentioned requirements in the CII Regulations, especially the requirement of setting up a specialized security management team for the protection of CII. We believe that such specialized security management team and its responsible person can also operate as the management team and responsible person required for the protection of important data and personal information under the Data Security Law and the Personal Information Protection Law, pending further clarification in practice.

Procurement of "Secure and Credible" Network Products and Services

The CII Regulations further require the operators to procure secure and credible network products and services and enter into confidentiality agreements with providers. Such confidentiality agreements need to clearly set forth the technical support and confidentiality obligations of the providers. The operators are required to supervise such providers with respect to the performance of their obligations under the agreement. If the procurement of relevant network products and services may have an impact on national security, the operators shall pass a security review in accordance with relevant national cybersecurity regulations. (Arts. 19, 20)

Note that there is no definition of "network products and services" under the CII Regulations. The Measures for Cybersecurity Review (MCR) provide some guidance on this topic. Under the MCR, the term "network products and services" refers to "core network equipment, high-performance computers and servers, large-capacity storage equipment, large databases and application software, network security equipment, cloud computing services, and other network products and services with a material impact on the security of CII." The draft amendment of MCR released in July 2021 added "important communication products" to the list. We believe that the scope of "network products and services" under the CII Regulations should be consistent with the MCR, pending further clarification.

We suggest companies that might be or are already considered to be CII operators review their contracts with their product and service providers and make sure that such contracts have clear confidentiality clauses. Also, we suggest conducting audits on such providers on a periodic basis. Such audits should focus on the providers' performance of their obligations under the above-mentioned contracts. Regarding network products and services that fall into the definition set forth in the MCR, we suggest that companies make a self-determination regarding the potential risk to the national security prior to the procurement and apply for cybersecurity review in accordance with the MCR if there is such a risk.

CII Protection Mechanism

According to the CII Regulations, the CAC shall coordinate with relevant departments to establish cybersecurity information sharing mechanisms; gather, study, evaluate, share, and release information, including cybersecurity threats, vulnerabilities, and incidents; and promote cybersecurity information sharing among relevant departments, Protection Departments, CII operators, and cybersecurity service providers. (Art. 23)

The Protection Departments shall establish and improve CII cybersecurity monitoring and warning mechanisms for their respective sectors, provide warnings and notifications on cybersecurity threats and hazards, and provide guidance on security protection. (Art. 24) In addition, the Protection Departments shall formulate cybersecurity incident emergency plans for their respective sectors, conduct emergency drills regularly, and provide guidance and technical support and assistance to CII operators in responding to cybersecurity incidents. (Art. 25)

The Protection Departments shall conduct cybersecurity inspection and testing on the CII in their respective sectors, provide guidance and supervise the operators as they make corrections, and improve security measures.

(Art. 26) The CAC shall be responsible for the overall coordination with respect to the inspection and testing conducted by the MPS and the Protection Departments. Such departments shall avoid unnecessary and repeated inspections. (Art. 27)

We suggest companies enhance their monitoring and warning mechanisms as well as emergency response mechanisms. Also, companies should cooperate as appropriate when the Protection Departments, public security authorities, and other relevant authorities conduct cybersecurity inspection and testing.

Legal Liabilities

Entities in violation of the CII Regulations may be subject to fines of up to RMB 1 million or 10 times the price of the procured network products and services, with fines of up to RMB 100,000 for directly responsible persons. Directly responsible persons of entities conducting illegal intrusion, disruption, and destruction of CII may be subject to administrative detention of up to 15 days. Fines of up to RMB 1 million may also be imposed concurrently. (Arts. 39-43)

It is noteworthy that individuals having received administrative penalties for activities jeopardizing the security of CII and for unapproved/unauthorized vulnerability detection and penetration testing shall not be allowed to engage in cybersecurity management or take key network operation positions within five years. Those individuals that have received criminal penalties shall not be permitted to engage in the above-mentioned activities ever again. (Art. 43)

Companies already identified as CII operators by the Chinese government should start working to fulfill their obligations under the CII Regulations as soon as possible. Those companies that are likely to be identified as CII operators should pay attention to the requirements of the CII Regulations and be prepared for any possible identification as CII operators in the future.

Explore more in

Privacy & Security

Related insights

Update

Wrapping Paper Series: Issues and Trends Facing the Retail Industry During the Holiday Season

Update

Privacy Law Recap 2024: Regulatory Enforcement