LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice September 2, 2021 | Number 2892

China Issues New Regulations to Protect the Critical Information Infrastructure

The regulations aim to protect the security of the CII and impose more compliance obligations in support of the Network Security Law.

Key Points:

The regulations are designed to provide clarification and guidance on:

- Scope and designation of the critical information infrastructure (CII)
- Compliance obligations for operators of the CII
- Regulatory requirements on the protection of the CII
- Penalties (including high fines and severe consequences) on operators of the CII that fail to fulfill the compliance obligations and to meet regulatory requirements

Background

On July 30, 2021, the State Council of the People's Republic of China (PRC) published the Security Protection Regulations on the Critical Information Infrastructure (the Regulations), which was passed by the State Council on April 27, 2021. The Regulations took effect on September 1, 2021, the same day the recently promulgated Data Security Law came into force.

The Regulations are the first set of administrative regulations promulgated by the State Counsel on the CII after the term "critical information infrastructure" was first introduced in the Network Security Law in 2016.

Definition and Identification of the CII

Article 31 of the Network Security Law generally defines the CII as infrastructure from important industries and sectors, including public communication and information services, energy, transportation, water conservancy, finance, public service, and e-government, as well as other industries and sectors that may pose severe threat to national security, people's livelihood, and public interests if their data is damaged or disabled or leaked. Article 31 of the Network Security Law further delegates to the State Council the authority to formulate specific regulations on the CII.

With the delegated authority, the State Council formulated the Regulations to offer an even broader definition of the CII and provide the methods and factors of designating the CII. According to Article 2 of the Regulations, the CII refers to critical network facilities and information systems from not only the important industries and sectors enumerated in the Article 31 of the Network Security Law as aforementioned, but also "national defense and technology industries."

Article 8 and Article 9 of the Regulations further delegate the competent industry regulators (i.e., the Protection Departments) the authority to: (1) formulate the implementing rules to designate the CII for their industries and sectors, and (2) take charge of the security protection of the CIIs in their industries and sectors. The Regulations note three factors when considering designation of the CII:

- The importance of infrastructure (including network facilities, information systems, etc.) to the core business of the industries and sectors
- The degree of severity if the infrastructure (including network facilities, information systems, etc.) is damaged or disabled, or if data is leaked
- The impact of the infrastructure on other industries and sectors

As required by the Regulations, the designation rules formulated by the Protection Departments, as well as the designated CIIs, shall be reported to the Public Security Bureau of the State Council for record.[1]

The Protection Departments must also notify designated critical information infrastructure operators (CIIOs) in a timely manner. If a CII has undergone significant changes that may affect the outcome of the designation, the CIIO should promptly update the Protection Departments on the relevant changes, and the Protection Department should undertake another assessment and designation within three months from the date of receiving the report, then notify the CIIO and the Public Security Bureau of the result of the re-designation.

It is commonly expected that the new CII definition and designation process may result in an even greater number of network operators to be designated as CIIOs than under the Network Security Law.

Compliance Obligations of CIIOs and Related Penalties

Compared to the Network Security Law, the Regulations impose more obligations on designated CIIOs, charge higher monetary fines, and hand down more severe consequences for failure to comply with the obligations.

A Comparison of the Network Security Law and the Regulations

The Network Security Law		The Regulations	
Obligations	**Penalties**	**Obligations**	**Penalties**
		Article 11: If any CII has undergone significant changes that may affect the designation results, the CIIO shall update the Protection Departments	**Article 39:** Non-compliant CIIOs may be required to rectify damage caused by violations and may receive a warning from competent authorities; CIIOs who

		promptly on the relevant changes	refuse to rectify, or cause severe network security consequences, may face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (~US$154,000), and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (US$15,000).
Article 33: The CII shall support stable and continuous business operations, and ensure security measures are designed, implemented, and used in tandem with the CII	**Article 59:** Non-compliant CIIOs may be required to rectify damage caused by violations and may receive a warning from competent authorities; CIIOs who refuse to rectify, or cause severe network security consequences, may face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (~US$154,000), and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (~US$15,000).	**Article 12:** CIIOs shall design, implement, and use security protection measures in tandem with the CII	
		Article 13: CIIOs shall establish a comprehensive network security protection system and accountability system	
Article 34: CIIOs shall set up a dedicated security management function	**Article 59:** Non-compliant CIIOs may be required to rectify damage caused by violations and may receive a warning competent authorities; CIIOs who refuse to rectify, or cause severe network security consequences, may face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (~US$154,000), and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and	**Article 14:** CIIOs shall set up a specified security management function	
Article 34: CIIOs shall designate a person to take charge of the security management department and shall carry out security background checks on key personnel		**Article 14:** CIIOs shall carry out security background checks on key personnel in the security management function, with support from the Public Security Bureau or National Security Bureau, as needed	

	CNY100,000 (~US$15,000).		
		Article 15: The security management function of the CIIO shall be responsible for the specific security protection works, including: (1) establishing and improving the network security management and evaluating system, and designing security protection plans for the CII; (2) increasing network security protection capacity, and carrying out network security monitoring, detection, and risk assessments; (3) formulating emergency plans, carrying out regular emergency drills, and dealing with network security incidents; (4) identifying key positions relating to network security, organizing network security working performance assessments, and proposing rewards and punishments for key personnel; (5) organizing network security education and training; (6) protecting personal information and data security, and establishing and improving the personal information and	

		data security protection system; (7) implementing security management for the design, construction, operation, and maintenance for the CII; and (8) reporting network security incidents and important matters in accordance with rules and regulations	
		Article 16: Personnel from the security management function shall be involved in decisions relating to network security	
Article 38: CIIOs shall carry out a network security inspection and risk assessment at least once a year, either on their own or via related service agencies, and submit the examination and assessment results as well as improvement measures to the competent authorities in charge of CII security	**Article 59:** Non-compliant CIIOs may be required to rectify damage caused by violations and may receive a warning from competent authorities; CIIOs who refuse to rectify, or cause severe network security consequences, may face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (~US$154,000), and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (~US$15,000).	**Article 17:** CIIOs shall carry out a network security inspection and risk assessment at least once a year, either on their own or via related service agencies, rectify identified security issues promptly, and report any issues as required by the Protection Departments	
Article 36: When purchasing network products and services, CIIOs shall enter into security confidentiality agreements with providers		**Article 20:** When purchasing network products and services, CIIOs shall enter into security confidentiality agreements with providers	
		Article 21: CIIOs shall report to the Protection Departments promptly regarding their mergers, divisions, or dissolution, and shall properly dispose	

		the CII as required by the Protection Departments	
		Article 18: CIIOs shall report significant network security incidents or threats to the CII to the Protection Departments and the Public Security Bureau	**Article 40:** Non-compliant CIIOs may be required to rectify damage caused by violations and may receive a warning from the Protection Departments and the Public Security Bureau; CIIOs who refuse to rectify, or cause severe network security consequences, may face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (~US$154,000), and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (US$15,000).
Article 35: If the purchase of network products and services may threaten national security, the National Network and Information Department, together with competent departments of the State Council, shall undertake a national security review	**Article 65:** Non-compliant CIIOs may be prevented from using such network products and services and face monetary penalties between one and 10 times the purchase value, and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (~US$15,000).	**Article 19:** CIIOs shall purchase safe and credible network products and services; if the purchase of network products and services may impact national security, a security review shall be conducted first[2]	**Article 41:** Non-compliant CIIOs may be required to rectify damage caused by violations and may receive a warning from related authorities under the Cybersecurity Administration of China, face monetary penalties between one and 10 times the procurement value, and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (~US$15,000).
		Article 28: CIIOs shall cooperate with the network security inspections carried out by the Protection Departments, the Public Security Bureau, the National Security Bureau,	**Article 42:** Non-compliant CIIOs may be required by related authorities to rectify damage caused by violations; CIIOs who refuse to rectify may face monetary penalties between CNY50,000 (~US$7,700) and CNY500,000 (~US$77,000), and

		and other governmental authorities	responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (US$15,000); CIIOs who have committed severe violations shall face criminal liabilities
Article 37: CIIOs shall store personal information and important data collected and generated in PRC during its operation within the territory of the PRC. If such information and data have to be transferred overseas for business purposes, security assessments shall be conducted.[3]	**Article 66:** Non-compliant CIIOs may be require to rectify damage caused by violations, receive a warning from the competent authority, face monetary penalties between CNY50,000 (~US$7,700) and CNY500,000 (~US$77,000), and may face suspension of any related business, winding up for rectification, website shutdown, and revocation of business license.		
Article 34: CIIOs shall provide practitioners with regular cybersecurity education, technical training, and skill assessments.	**Article 59:** Non-compliant CIIOs may be required to rectify damage caused by violations and may receive a warning from competent authorities; CIIOs who refuse to rectify, or cause severe network security consequences, may face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (~US$154,000), and responsible personnel may be subject to fines between CNY10,000 (~US$1,500) and CNY100,000 (~US$15,000).		
Article 34: CIIOs shall ensure important systems and databases are backed up			
Article 34: CIIOs shall implement emergency plans for cybersecurity events and carry out routine emergency drills			
Article 34: CIIOs shall perform other obligations provided for in relevant laws and			

administrative regulations			

Obligations and Penalties Imposed on Parties Other Than CIIOs

To further protect the security of the CII, the Regulations also impose requirements and penalties on other parties.[4] In particular, the Regulations prohibit any entity or individual from conducting unauthorized loophole detection, permeability tests, etc. without proper pre-approval from the Protection Department or advanced consent from the CIIOs. The Regulations specify that all entities and individuals shall not:

- Illegally invade, interfere with, or destroy the CII, and shall not endanger the security of the CII. Non-compliant individuals will face confiscation of illegal gains, administrative detention of no more than five days, and may face monetary penalties between CNY50,000 (~US$7,700) and CNY500,000 (~US$77,000). Individuals who have committed severe violations will face administrative detention between five and 15 days and may face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (US$154,000). Non-compliant entities will face confiscation of illegal gains and will face monetary penalties between CNY100,000 (~US$15,000) and CNY1 million (~US$154,000). Responsible personnel may also be subject to penalties. Individuals receiving administrative penalties shall not be allowed to work in key positions relating to the network security management and network operations for five years, and individuals receiving criminal penalties shall not be allowed to work in such positions for the rest of their lives.

- Carry out loophole detection or permeability tests on the CII that may affect or endanger the security activities of the CII, without pre-approval from the competent government authorities. Non-compliant individuals receiving administrative penalties shall not be allowed to work in key positions relating to the network security management and network operations for five years, and individuals receiving criminal penalties shall not be allowed to work in such positions for the rest of their lives.

Governmental Authorities' Responsibilities and Duties

The Regulations outline responsibilities and duties for related governmental authorities (including the Protection Departments) to carry out the security protection of the CII.

The Protection Departments are required to:

- Plan the security of the CII in their industries and sectors, and clarify the purpose, basic requirements, and specific measures of this protection

- Establish the network security monitoring system for the CII in their industries and sectors, understand operational and security status of the CII, and notify network security threats and risks

- Establish emergency plans for the network security incidents, routinely organize emergency drills, and provide necessary support for CIIOs

The Cybersecurity Administration of China are responsible for:

- Coordinating with relevant departments to establish a network security information sharing mechanism; aggregate, research, share, and publish information promptly on network security threats, loopholes, and incidents; promote network security information sharing among related authorities, the Protection Departments, and CIIOs

- Coordinating with the Public Security Bureaus and the Protection Departments to carry out inspections on the network security of CII and propose improvement measures

The Public Security Bureaus and the National Security Bureaus are responsible for the security guidance of the CII, and to prevent and fight against criminals that target or exploit the CII.

Relevant authorities at provincial levels shall implement security protection, supervision, and management of the CII, according to their respective responsibilities.

Conclusion

The Regulations are expected to profoundly impact network operators, since more network operators may be designated as CIIOs while the competent authorities for the important industries and sectors work through their process for formulating the designation criteria and designate CIIs for their industries and sectors. Given the extensive compliance obligations and severe penalties imposed on CIIOs, all the network operators in those identified industries are advised to pay close attention to the work of their industry regulators and, if they have concerns that they might fall within the scope of CII, begin to improve their compliance programs in accordance with both the Regulations and the Network Law.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Hui Xu
hui.xu@lw.com
+86.10.5965.7006
Beijing

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

This *Client Alert* was prepared with the assistance of Esther Zheng in the Shanghai office of Latham & Watkins and Yuzheng Liang in the Beijing office of Latham & Watkins.

You Might Also Be Interested In

China's New Data Security Law: What to Know

China Issues Draft Data Security Law for Public Comment

Extensive Changes to Singapore's Data Protection Regime Take Effect

Hong Kong Considers Sweeping Changes to Privacy Laws

Endnotes

[1] According to the Guidance on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System, issued by the PRC Ministry of Public Security in 2020, infrastructure networks, large private networks, core business systems, cloud platforms, big data platforms, internet of things, industrial control systems, intelligent manufacturing systems, new internet, emerging communication facilities, and other key facilities may be considered as the CII.

[2] According to the Network Security Review Measures issued by the Cybersecurity Administration of China and other governmental authorities in 2020, the Office of Network Security Review established under the Internet Information Office of China is responsible for developing network security review-related norms and organizing network security review.

[3] For the cross-border transmission of data in CII, Article 31 of the Data Security Law stipulates that important data collected and generated by CIIOs in China shall refer to the provisions of the Network Security Law, which requires a security assessment pursuant to the measures developed by the Cyberspace Administration and competent departments of the State Council. This provision for cross-border data transfer was emphasized in the official Q&A issued by the Ministry of Justice, the Cybersecurity Administration, the Ministry of Industry and Information Technology, and the Ministry of Public Security of PRC on August 17, 2021.

[4] According to an official minutes issued by State Council on August 24, 2021, the spokesman of Cyberspace Administration further explained both domestic and foreign-funded enterprises, whether they are listed or not, and whether they are listed in PRC or overseas, shall protect CII security, as well as national network security and personal information security.