V&T LAW FIRM
万商天勤律师事务所

上海市浦东新区世纪大道 88 号金茂大厦 32 层 200120
电话：+86 21 50819091 www.vtlaw.cn
北京 深圳 上海 成都 武汉 西安 长沙 杭州 海口 南京 广州

China's GDPR?

A Quick Legal Review on the Recent CII Regulation

August 22, 2021
Foreign investment; cybersecurity compliance

Introduction

Cyber security, personal information, and data protection **("Cybersecurity Compliance")** have become a barbecue stopper recently in China, since the largest ride-hailing company in China has hit the headline when they decided to seek an overseas listing.

On August 20, 2021, the 30th session of the Standing Committee of the 13th National People's Congress passed the ***Personal Information Protection Law of the People's Republic of China***, which will come into force on November 1, 2021.[1] Just three days ago, on August 17, 2021, the State Council of China published the ***Regulation on Protection of Security of Critical Information Infrastructure*** (**"CII Regulation"**) aiming to provide more detailed rules on the protection of China's critical information infrastructure (**"CII"**), and it will be officially implemented on September 1, 2021.[2] The CII regulation, as a core supporting administrative regulation of China's Cyber Security Law (**"CSL"**), elaborates on the definitions of the CII and sets the enhanced security obligations and requirements for CII operators (**"CIIO"**) compliance.[3] China seems to embrace a far-reaching new era of Cybersecurity Compliance.

With the implementation of the above laws and regulations, it would significantly affect the companies which operate CIIs as well as their domestic and overseas suppliers. To understand CIIOs risk exposures and statutory obligations in conformity of Cybersecurity Compliance, it would be possible for CIIOs to avoid facing criminal penalties or administrative detentions in case of failure to comply or violating CII-related laws and regulations. Given more onerous obligations and legal consequences on CIIOs, this article provides you with a quick understanding in this regard.

What is Critical Information Infrastructure?

[1] The 30th session of the Standing Committee of the 13th National People's Congress passed the Personal Information Protection Law of the People's Republic of China, available at http://www.xinhuanet.com/politics/2021-08/20/c_1127779295.htm

[2] The State Council of China published the Regulation on Protection of Security of Critical Information Infrastructure, available at: http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm

[3] See Cyber Security Law of People's Republic of China, available at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

Article 2 of the **CII Regulation** defines CII as: *"Important network facilities, information systems, etc. in important industries and fields such as public communications and information services, energy, transportation, water, finance, public services, e-government affairs and defense technologies, which, in the event of damage thereto, loss of function thereof or leak of data therefrom, could seriously jeopardize national security, national economy, and people's livelihoods, or the public interest."* [4]

To determine what is CII, there are two elements for CII: (1) it is in the crucial industries and fields, and (2) the consequences in case of damage thereto, loss of function thereof or data leakage therefrom is harmful and severe. It's also important to note that the definition of CII is not exhaustive in terms of important industries and fields. It therefore allows authorities to have a broad discretionary power to make other so-called non-crucial network facilities and information systems, whose failure could harm national security, national economy, or public interest, fall into the definition of CII. Set forth below is the definition of CII in a tabular form for illustration purposes:

No.	The Elements of Identification	CII Regulation
1	The industries and the fields	Public communications and information services, energy, transportation, water, finance, public services, e-government affairs, and defense science and technology industry and other important industries and fields.
2	The harm of the failure	In the event of damage thereto, loss of function thereof or leak of data therefrom, could seriously jeopardize national security, national economy, and people's livelihoods, or the public interest.

Who is a CII Operator?

CII Regulation leaves the authority to define who is CIIO to allow the regulators or administrative and supervisory authorities of the critical industries and fields under *Article 2* (**"the Guardian Authorities"**) to define the scope of the CIIO.[5] If a company is identified as CIIO, the Guardian Authorities will notify the company about such identification and its

[4] See Article 2 of CII Regulation.
[5] See Article 8 of CII Regulation.

related statutory obligations of CIIO for compliance purposes.

Specifically, **CII Regulation** provides that the Guardian Authorities could implement the following procedures and have the power to identify a CIIO:

(1) Formulate their own rules for identifying CII within their respective purviews (the identification rules), taking into consideration the following factors:[6]
  (a) The importance of the network facilities, information systems, etc. to the key businesses of the relevant industries or fields;
  (b) The harm that may be caused by the damage to, loss of function of or dissemination of data from the network facilities, information systems, etc; and
  (c) Associated impact to other industries and fields.

(2) Be responsible for identifying the CII in their respective purviews in accordance with the identification rules and notifying to Public Security Department of the State Council the results of their determination.[7]

(3) Make a new identification when CII changes greatly and affects the identification.[8]

Legal Consequences if a CIIO Fails to Comply?

CIIOs shall be subject to perform their statutory obligations under CII Regulation and CSL. In failure of compliance, CIIOs may face a variety of penalties, and their person-in-charge and other responsible individuals may also be personally liable according to CII Regulations and CSL. In the worst case scenario, such as incidents concerning national security, criminal liability would be triggered and imposed. Legal consequences of violating CII Regulation and CSL includes but not limited to the following:

1. Criminal Liability

Even though CII Regulation does not directly include criminal liability or criminal penalty-related provisions, yet the occurrence of major security accidents may reference to the relevant provisions in Chinese criminal law, therefore, a CIIO and the person-in-charge and other responsible individuals may need to be aware of criminal penalties therefrom.[9]

2. Administrative Detentions and Injunctions

Any person or a CIIO who illegally invades, disturbs, or destroys CII, or carry out

[6] See Article 9 of CII Regulation.
[7] See Article 10 of CII Regulation.
[8] See Article 11 of CII Regulation.
[9] See Article 44, 45, 46, 47, 48 of CII Regulation.

vulnerability detection, permeability testing, and other activities that may affect or endanger the security of CII without prior approval from the Guardian Authorities may face (i) administrative detention which could be up to 15 days, or (ii) a five-year to a life-time injunction to perform as a CIIO according to Article 43 of the CII Regulation.[10]

3. Administrative Fines

The administrative fines could be imposed, which range from RMB 50,000 up to one million or even ten times the procured price of the network product or service.

- A fine of not less than RMB 100,000 but not more than one million would be imposed upon a CIIO under the following circumstances, and the person-in-charge shall also be fined from RMB 10,000 to RMB 100,000:[11]
  (1) Failing to timely report relevant information when major changes have taken place in the infrastructure which may affect the rectification of CII regarding the infrastructure;
  (2) The security protection measures are not synchronically constructed and applied to CII;
  (3) Failing to establish a CII security protection system and responsibility system;
  (4) Failing to establish a special safety management system for CII;
  (5) Failing to conduct safety background investigation regarding the important CII operating personnel;
  (6) Making decisions related to CII security without the participation of personnel of CII management-related institutions;
  (7) Failing to perform the duties of secure CII, including drafting plans, conducting risk assessments, etc.;
  (8) Failing to conduct an annual risk assessment for CII or failing to report the risk as required;
  (9) Failing to comply with the purchase agreements of network products in accordance with relevant state regulations;
  (10) Failing to timely report the merger, division, or dissolution of CII as required; and
  (11) Failing to report major security incidents or threats that occurred to CII as required.

- A fine up to a 10-time procured price of the network product or service would be imposed when the procured network products and services would possibly jeopardize national security and could not pass the national cybersecurity review, and the person-in-charge would also be fined from RMB 10,000 to RMB 100,000.[12]

[10] See Article 43 of CII Regulation.

[11] See Article 39, 40 of CII Regulation.

[12] See Article 41 of CII Regulation.

- A fine of RMB 50,000 to RMB 500,000 would be imposed if a CIIO is reluctant to cooperate with the Guardian Authorities to conduct CII inspection of risk assessment, and the relevant personnel would also be fined up to RMB 100,000.[13]

4. Other Administrative Punishments

Additionally, under CSL, the requirements for data export and procurement of network devices and services would be stricter for CIIOs than that of CII Regulation. In accordance with CSL, besides imposing a fine, the competent Guardian Authorities may order a CIIO in term of violation or failure to comply to (i) rectify their wrong-doings, (ii) give them a warning, (iii) confiscate their illegal income, (iv) suspend relevant businesses, (v) suspend business operations, (vi) close down websites, or (vii) revoke relevant business licenses.

Suggestions on CIIOs' Compliance

Given more onerous obligations and legal consequences on CIIOs, we offer the following suggestions that may guide CIIOs through rough patches when they operate in China:

1. Systematically Protecting the Security of CII

To put the security protection of CII in a prime position is the very first advice: comprehensively engineer the CII projects as a whole picture from the beginning of the construction and systematically operate the CII with security protection measures throughout the entire process.

2. Establishing and Improving the Responsibility System of CII Protection

When it comes to CII protection, CIIOs are advised to put in place sufficient manpower, materials, and finances. In terms of protecting CII and coping with major security incidents, the person-in-charge of CII is obliged to shoulder the duty of leading from the front.

3. Establishing a Security Management Institution and Perfect Basic Training and Security Education

CIIOs should establish a special security management institution, as well as to conduct security background checks on the person-in-charge and the key staff of such institution. CIIOs should improve their own CII security management system, formulate CII security protection plans, make their own emergency response plans (in accordance with national

[13] See Article 42 of CII Regulation.

上海市浦东新区世纪大道 88 号金茂大厦 32 层 200120
电话：+86 21 50819091 www.vtlaw.cn
北京 深圳 上海 成都 武汉 西安 长沙 杭州 海口 南京 广州

and industry CII security incident emergency plans), and organize regular emergency exercises and CII security education and training.

4. Regularly Conducting Cybersecurity Testing and Risk Assessment

CIIOs are advised to conduct cybersecurity testing and risk assessment at least once per year (either on their own or by entrusting facilitating agencies), rectify the security issues uncovered in the testing or assessment and prepare reports in accordance with the requirements of the Guardian Authorities.

5. Proactively Fulfilling the Obligations of Reporting Major Issues

When a major security incident occurs or a major security threat is discovered in CII, CIIOs shall immediately report to the Guardian Authorities in accordance with relevant regulations. In particular, it is advised to report to the Cyberspace Administration of China (the **"CAC"**) and the Ministry of Public Security (the **"MPS"**) if there occurs overall interruption of operation, major functional failures, leakage of national basic information, and other important data, leakage of large-scale personal information, extremely major cybersecurity incidents bringing about large economic losses and large-scale dissemination of illegal information, or special security threat.

6. Proactively Fulfilling the Obligation of Reporting Changes

A CIIO should notify the Guardian Authorities in the event of a merger, division, or dissolution of the CIIO, and disposal of the CII in accordance with the requirements of the Guardian Authorities in order to ensure safety.

7. Proactively Fulfilling the Obligations During the Procurement

A CIIO should prioritize secure and reliable network products and services in procurement; if national security may be concerned by the procurement of network products or services by the CIIO, a security review must be passed.

Given the complexity of CII related compliance, it is fairly critical for CIIOs to adopt active, or even proactive approaches to comply with the CII Regulation and CSL. To that end, constantly seeking legal advice for necessary precautions is strongly recommended and encouraged.

Author

Lyon Dong (Partner, head of cross-border business transaction department)	+86.13918921698	lyon.dong@vtlaw.cn
Joanna Fan (Senior Associate)		joanna.fan@vtlaw.cn
Cyrus Cao (Associate)		cyrus.cao@vtlaw.cn

Interns Keyuan Song (Class 2023 of Shanghai International Studies University), and Jingyi Hu (Class 2021 of University College London) also made contribution to this client alert.

Contact

If you have any questions about this client alert, or if you would like to discuss how recent changes in Chinese law may affect your business, please call or write:

Lyon Dong (Partner) +86. 13918921698 lyon.dong@vtlaw.cn

32nd Floor, Jinmao Tower, 88 Century Avenue, Pudong, Shanghai 200120, China

Disclaimer