



PRC Promulgated Regulations on the Security Protection of Critical Information Infrastructure

Dear Sir or Madam,

On 30 July 2021, the PRC State Council, 4 years after the draft had been published, finally adopted the *Regulations on the Security Protection of Critical Information Infrastructure* ("CII Regulations"). They will take effect on 1 September 2021. The CII Regulations provide more detailed and practical guidance than the stipulations of the *PRC Cybersecurity Law* regarding the scope, identification rules, obligations of critical information infrastructure operators and corresponding liabilities in case of violation of critical information infrastructure. Please find below a brief of the new regulations.

Kind regards,
CMS, China

The PRC State Council on 30 July 2021 finally adopted the *Regulations on the Security Protection of Critical Information Infrastructure* ("CII Regulations"). They will take effect on 1 September 2021.

1. Background

The *PRC Cybersecurity Law* ("CSL") introduced the concept of critical information infrastructure ("CII") and emphasizes that stronger protection shall be provided for CII, but does not provide detailed measures for carrying out such specific protection. The scope of CII and detailed measures for protecting security of CII shall be formulated by the State Council afterwards. The CII Regulations were published for public comments already on 10 July 2017. It took four years until they were now officially promulgated on 30 July 2021. The CII Regulations and the CSL establish the overall structure of identification and supervision of CII and clarify specific obligations of critical information infrastructure operators ("CIIOs").

2. Key Aspects in the CII Regulations

The CII Regulations cover the following key aspects:

- Overview of the CII Regulations;
- Identification rules for CII;
- Obligations of CIIOs;
- Guarantee and Advancement of security protection for CII;
- Liabilities for violation of CIIOs' obligations.

3. Overview of the CII Regulations

a) Definition of CIIs

According to Article 2 of the CII Regulations, CIIs refer to key network facilities and informational systems in important industries and sectors such as public telecommunication and information service, energy, transport, water conservancy, finance, public service, e-government and science and technology industries for national defense, 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. Compared with the definition under Article 31 of the CSL, the CII Regulations add one additional important industry, i.e. science and technology industry for national defense, and clarify that the objects of CIIs are important network facilities and informational systems. This seems to imply that even if the business system of an enterprise is identified as a CII, this does not mean that other systems of the enterprise, such as employee system, financial system and other operating systems of the enterprise which are not associated with the main business system, are automatically identified as CIIs accordingly.

b) Competent authorities

Article 3 of the CII Regulations clarifies the responsibility of relevant authorities involved in the regulation of CIIs. The national cyberspace department will coordinate the interaction of different authorities. The public security department under the State Council is responsible for guiding and supervising the security protection of CIIs. In addition, the telecommunication department and other relevant departments under the State Council will be responsible for supervision and management of security protection of CIIs within the scope of their respective duties in accordance with the relevant regulations and laws. Further, relevant departments of the provincial governments shall supervise and manage the security protection of CIIs according to their respective duties. Therefore, if certain network facilities or informational systems are identified as CIIs, they will be subject to various regulations formulated by the above different authorities.

4. Identification Rules for CIIs

Article 8 of the CII Regulations provides that the supervision and management authorities of the important industries and sectors mentioned in Article 2 ("CII Protection Departments") are responsible for security protection of CIIs. According to Article 9 of the CII Regulations, the respective CII Protection Departments shall formulate the identification rules for CIIs based on the actual situation in a specific industry or sector. Therefore, detailed identification rules from specific CII Protection Departments are expected to be formulated in the near future. Nevertheless, the CII Regulations provide the following general identification factors and procedures for reference.

a) Identification factors

According to Article 9 of the CII Regulations, the following factors shall be taken into consideration for formulating identification rules:

- (1) The degree of importance of the network facilities and information systems to the core business in the specific industry and sector;
- (2) The degree of harm which may be brought once the network facilities and information systems are subject to any destruction, loss of function or data leakage;
- (3) The correlative impact on other industries and sectors.

b) Identification procedures

First, the CII Protection Departments shall record the specific identification rules at the public security department under the State Council according to Article 9 of the CII Regulations.

Further according to Article 10 of the CII Regulations, the CII Protection Departments shall be responsible for identifying the CIIs in their respective industries and sectors in accordance with the formulated identification rules, timely notify the relevant operators of the identification results and meanwhile report the same to the public security department under the State Council.

If there are major changes of the CIIs which are likely to affect the identification results, the relevant operators shall timely report to the CII Protection Departments according to Article 11 of the CII Regulations. The CII Protection Departments shall conduct the identification once again within three months upon receipt of the report, notify the network operators of the identification results and report the same to the public

5. Obligations of CIIOs

The relevant network operators who operate the CIIs are referred to as the CIIOs and shall undertake corresponding obligations. Similar with the CSL, the CII Regulations stipulate that CIIOs shall establish an overall cybersecurity protection system and clearly allocate internal responsibility of cybersecurity in case of violation. In details, the following obligations of CIIOs shall be fulfilled according to the CII Regulations:

a) General obligations

(1) Designation of a specific security management organ

According to Article 14 of the CII Regulations, CIIOs shall set up a specific security management organization and conduct background examination of the person-in-charge and relevant persons in key positions of the said organization. Further, the public security departments and national security departments shall provide assistance in such background examination.

For supporting the specific security management organization, Article 16 of the CII Regulations provides that CIIOs shall guarantee sufficient operational expenses and appoint relevant personnel. In addition, any decision-making process which is related to cybersecurity and information technology application shall have participation of the personnel from the specific security management organization.

(2) General duties of the specific security management organization

After the designation of a specific security management organ, Article 15 of the CII Regulations specifically provides that the specific security management organ shall fulfil the following duties:

- Establishing and improving cybersecurity management, evaluation and assessment system, and formulating the CII security protection plan;
- Organizing and advancing the capacity of cybersecurity protection and conducting cybersecurity monitoring, detection and risk assessment;
- Formulating contingency plans in case of cybersecurity incidents in accordance with national and industrial contingency plans, carrying out regular emergency drills and effectively handling cybersecurity incidents;
- Identifying key positions involving cybersecurity, organizing and carrying out cybersecurity work assessment, and giving opinions on commendation and punishment;
- Organizing cybersecurity-related education and training;
- Performing duties in personal information protection and data security protection, and establishing and improving a sound system for personal information and data security protection;
- Implementing security management for the design, construction, operation, maintenance and other services involving CIIs;
- Reporting cybersecurity incidents and important matters as required.

(3) Report obligations

- According to Article 11 of the CII Regulations as introduced above, CIIOs are always obliged to timely report any changes of CIIs which may affect the identification results of CIIs to the CII Protection Departments.
- Article 17 of the CII Regulations provides that CIIOs shall carry out cybersecurity testing and risk assessment of the CIIs at least once a year by themselves or entrusting cybersecurity service agencies, rectify any security problems discovered in a timely manner, and report the situation in accordance with the requirements of the CII Protection Departments.
- Article 18 of the CII Regulations provides that, in the event of a serious cybersecurity incident or serious cybersecurity risks, CIIOs shall report to the CII Protection Departments and the public security department in accordance with the relevant provisions.

- Further, in case of merger, separation, dissolution, etc., CIIOs shall promptly report the same to the CII Protection Departments and dispose of the CIIs in accordance with the requirements of the CII Protection Departments according to Article 21 of the CII Regulations.

b) Security review on third parties' network products and services

For purchasing network products and services provided by any third parties, Article 19 of the CII Regulations emphasizes that CIIOs shall give priority to procuring safe and credible network products and services. If the third parties' network products and services may affect national security, the network products and services shall pass a security review in accordance with relevant provisions regarding national cybersecurity.

In addition, Article 20 of the CII Regulations provides that CIIOs shall enter into security confidentiality agreements specifying the provider's technical support and security confidentiality obligations with the provider for purchasing the network products and services. Further, the CIIOs shall supervise the performance of the relevant obligations.

c) Cooperation with cybersecurity inspection conducted by relevant authorities

Since the CII Regulations aim to implement stricter regulation on CIIOs than on normal network operators, relevant authorities are authorized to inspect the cybersecurity of CIIs. Article 28 of the CII Regulations provides that CIIOs shall cooperate with cybersecurity inspection and detection conducted by the CII Protection Departments as well as the public security department, national security department, confidentiality administration department, cryptography administration and relevant departments in accordance with the law.

6. Guarantee and Advancement of Security Protection for CIIs

a) Prohibition of vulnerability detection test without approval or authorization

Article 31 of the CII Regulations provides that any individual or organization shall not implement vulnerability detection, penetration testing and other activities which may affect or endanger the security of CIIs without approval of the national cyberspace department, the public security department under the State Council or authorization of the CII Protection Departments and the CIIOs. In addition, the implementation of network vulnerability detection, penetration testing and other activities on the basic telecommunication networks shall be reported to the telecommunication department under the State Council in advance.

As a result, any network vulnerability detection, penetration testing and other activities on the CIIs without approval or authorization are likely to constitute illegal invasion of CIIs in violation of Article 43 of the CII Regulations, which may be subject to administrative penalties (such as fines and detention) or even criminal punishment. Further, the individual who is subject to administrative penalties shall be prohibited from undertaking key positions related to cybersecurity management and operation for five years, and the individual who is subject to criminal punishment shall be prohibited from undertaking key positions related to cybersecurity management and operation for his or her whole lifetime.

b) Restrictions on the relevant authorities

In addition to the obligations of CIIOs, the CII Regulations provide certain restrictions on the relevant authorities' power in order to protect CIIOs' legal rights.

- Article 27 of the CII Regulations stipulates that the relevant authorities shall not charge any fees for carrying out cybersecurity inspection and shall not require the CIIOs to purchase products and services of a specified brand or a designated producer or seller.
- Further, according to Article 30 of the CII Regulations, any information obtained in the process of the security protection of CIIs by the cyberspace department, public security department, CII Protection Departments and other relevant departments, as well as cybersecurity service agencies and their staffs can only be used for the purpose of safeguarding cybersecurity. The above authorities, agencies and individuals shall ensure the security of relevant information strictly in accordance with the relevant laws and regulations, and shall not disclose, sell or illegally provide the same to others.

7. Liabilities for Violation of CIIOs' Obligations

a) Liability for violation of general obligations

Article 39 of the CII Regulations stipulates corresponding liability for an exhaustive list of violation circumstances. The list of violation circumstances covers the general obligations of CIIOs (as stated in above Item 5 a)) and the specific obligation of entering into a security confidentiality agreement with network products and services providers (as stated in above Item 5 b)). In case of violation, the CIIOs shall be ordered by the relevant competent departments to make rectification and given warnings. If a CIIO refuses to make rectification or cause harmful consequences to cybersecurity, the CIIO shall be imposed with a fine of no less than RMB 100,000 but no more than RMB 1 million. The persons directly in charge shall be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000.

Article 40 of the CII Regulations specifically addresses the liability for failure of reporting serious cybersecurity incidents or risks (as stated in above Item 5 a) (3)). In the event of violation of the above obligations, the liabilities are the same as stated in the preceding paragraph, while the competent authorities are specified as the CII Protection Departments.

b) Liability for not conducting security review of a third party's network products and services

If the CIIOs purchase network products or services which may affect national security without conducting the security review pursuant to Article 19 (as stated in above Item 5 b)), Article 41 of the CII Regulations provides that the CIIOs shall be ordered by the national cyberspace department and other relevant departments to make rectification and be imposed with a fine of no less than one but no more than ten times the purchase amount. In addition, the persons directly in charge or other directly responsible persons shall be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000.

c) Liability for not cooperating with cybersecurity inspection conducted by relevant authorities

If the CIIOs do not cooperate with cybersecurity inspection conducted by relevant authorities pursuant to Article 28 (as stated in above Item 5 c)), Article 42 of the CII Regulations provides that the CIIOs shall be ordered by relevant competent departments to make rectification. If a CIIO refuses to make rectification, they will be imposed with a fine of no less than RMB 50,000 but no more than RMB 500,000. The persons directly in charge or other directly responsible persons shall be imposed with a fine of no less than RMB 10,000 but no more than RMB 100,000. In the event of serious circumstances, the CIIO shall be subject to other legal liabilities.

8. Conclusion

In conclusion, the CII Regulations provide more detailed and practical guidance than the stipulations of the CSL regarding scope, identification rules, obligations of CIIOs and corresponding liabilities in case of violation. The key question is whether certain network facilities and informational systems qualify as CIIs. However, the exact parameters are still unclear for the time being because the specific identification rules in important industries and sectors have not yet been promulgated and the identification of CIIs is likely to be determined on a case-by-case basis in the future. As the identification rules will be formulated by the respective CII Protection Departments for specific industries and sectors, we recommend that relevant enterprises engaging in the key industries, such as public telecommunication and information service, energy, transport, water conservancy, finance, public service, e-government and science and technology industry for national defense, shall keep close watch on the detailed identification rules for CIIs in the respective industries and sectors.

In case you have questions or for further information, please contact the authors of this newsletter:



Panpan Tang

Associate
CMS, China

T +86 21 6289 6363
E panpan.tang@cmslegal.cn



Spring Zhu

Junior Associate
CMS, China

T +86 21 6289 6363
E spring.zhu@cmslegal.cn

About CMS, China

关于 CMS, 中国

CMS is one of the top 10 global law firms. With more than 4,800 professional legal and tax advisors in over 70 offices in more than 40 countries, we advise clients on both global and local matters and provide pragmatic and commercial advice.

CMS, China has been advising clients on doing business in China for several decades. As one of the top international law firms in China, we are able to support international companies and Chinese enterprises on all their legal needs through our full service offering. We advise in the areas of M&A, corporate restructuring, FDI, distribution and commercial, competition, compliance, employment, banking and finance, insurance, real estate and construction, technology licenses, IP registration and enforcement, dispute resolution as well as tax and customs.


Our team of legal experts are from China, Germany and the UK, and have an in - depth knowledge and understanding in many industrial sectors such as automotive, manufacturing, machinery and equipment, life sciences and healthcare, energy, banking & finance and TMC. We focus on serving the needs of our clients and on providing them with solution driven and business-oriented advice.

作为全球最大的法律与税务服务机构之一，CMS 通过旗下遍布于 40 多个国家超过 70 个办公室的 5,000 多名律师，提供覆盖全球及本土化的商业可行性解决方案。

如今，CMS 在中国服务客户已有数十年的历史。作为中国最大的外资律所代表处之一，CMS, 中国专注于并购、公司重组、外商直接投资、分销和商法、竞争法、合规、劳动法、银行 和金融、保险、房地产和建筑、技术许可、知识 产权注册与执行、争议解决及税务和海关等各个领域， 为国际与中国公司提供全方位的法律咨询服务。


我们的顾问团队由来自中国、德国和英国的专家组成，对汽车、制造、机械设备、生命科学和医疗保健、能源、银行金融以及技术、传媒与通讯等行业领域有着全面深入的了解。我们注重为客户提供实际有效的咨询和解决方案， 以帮助客户达到既定商业目标。

 3108 Plaza 66, Tower 2, 1266 Nanjing Road West, Shanghai 200040 P.R.China
上海市南京西路 1266 号恒隆广场 2 期 3108 室

 Phone/ 电话: + 86 21 6289 6363

Fax/ 传真: + 86 21 6289 0731

 Web/ 网址: <https://cms.law/en/chn/>

 Email/ 电邮: info@cmslegal.cn



Welcome to follow our WeChat account where you will find the updated legal insights and news.

欢迎扫码关注我们的微信公众号，在这里您可以获取最新的法律资讯和新闻。