君合研究简讯

JUNHE

2017 年 7 月 14 日

网络安全法律热点问题

《关键信息基础设施安全保护条例》征求意见

国家互联网信息办公室（以下简称“**网信办**”）于 2017 年 7 月 11 日公布了《关键信息基础设施安全保护条例（征求意见稿）》（以下简称“**《征求意见稿》**”），为期一个月公开征求意见。

《网络安全法》（以下简称“**《网安法》**”）第一次引入了关键信息基础设施概念。根据《网安法》第 31 条规定，其范围和安全保护办法由国务院制定。而根据《国务院办公厅关于印发国务院 2016 年立法工作计划的通知》，《关键信息基础设施安全保护条例》由网信办起草。鉴于《网安法》生效已逾一月，关键信息基础设施作为《网安法》的核心议题之一，对其范围和保护措施进一步规范的《征求意见稿》的发布确实刻不容缓。《征求意见稿》之中对于网络安全的政府协调预警机制等方面均进行了全面的要求和规范。以下我们主要将《征求意见稿》之中可能对于企业的合规工作特别相关的条款进行总结。

一、 细化关键信息基础设施的适用范围

《网安法》将关键信息基础设施概括地定义为：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。”该定义建立了判断关键信息基础设施的两项基本标准：行业标准和后果标准。

《征求意见稿》第 18 条延续了《网安法》的判断标准，同时更明确的突出了后果标准，细化和更新了行业标准，其规定：“下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：

1、 政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

2、 电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；

3、 国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

4、 广播电台、电视台、通讯社等新闻单位；

5、 其他重点单位。”

相比《网安法》，《征求意见稿》的行业标准新增了“国防科工、大型装备、化工、食品药品”等类别。

同时，《征求意见稿》细化了“公共通信和信息服务”、“公共服务”等行业类别。其中，“公共服务”进一步细化为“卫生医疗、教育、社保、环境保护、公用事业”；“公共通信和信息服务”被细化为“电信网、广播电视网、互联网，提供云计算、大数据和其他大型公共信息网络服务的单位、广播电台、电视台、通讯社”等具体单位类型。

根据《征求意见稿》第 19 条规定，国家网信部门将会同电信主管部门、公安部门等制定关键信息基础设施识别指南，行业主管或监管部门根据识别指南组织识别本行业、本领域的关键信息基础设施并按程序报送识别结果。在实务之中，虽然《征求意见稿》的规定相关对《网安法》有进一步的细化，但具体的范围和判定标准则仍有待于识别指南的出台。《征求意见稿》相对笼统的规定也保留了后续执法和实践变化的灵活性。

二、重述关键信息基础设施运营者的安全保护义务

《征求意见稿》第 5 条明确规定，关键信息基础设施运营者（以下简称“**运营者**”）对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务。

《网安法》第 31 条和《征求意见稿》第 6 条均规定，关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。关键信息基础设施运营者（以下简称“**运营者**”）也属于网络运营者，因此其应当同时遵守《网安法》对于网络运营者和关键信息基础设施运营者的安全保护要求。

《征求意见稿》第四章重复了《网安法》的相关规定，包括要求运营者：

1、 建立内部安全制度、操作规程、严格的身份认证和权限管理；

2、 采取技术措施，防止危害网络安全行为、监控网络运行；

3、 采取数据分类、重要数据备份、加密认证等措施；

4、 设置专门的网络安全管理机构及负责人；

5、 对员工进行培训、技能考核；

6、 制定应急预案并定期演习；

7、 每年至少一次风险隐患检测评估；

8、 个人信息和重要数据境内存储。

相比《网安法》，《征求意见稿》提出了更细节的要求，包括：运营者网络安全关键岗位专业技术人员应实行持证上岗制度（具体规定尚未出台）；对员工的培训每人每年时长不得少于 1 个工作日；关键岗位专业技术人员进行每人每年时长不得少于 3 个工作日；关键信息基础设施上线运行前或发生重大变化时应当进行安全检测评估等。

三、加强网络产品和服务采购的检查和报告义务

《征求意见稿》在网络产品、服务安全方面重述了《网安法》的多项要求，包括：网络产品、服务应符合国家强制性要求；运营者采购网络产品和服务，可能影响国家安全的，应当通过网络安全审查，与提供者签订安全保密协议等。

《征求意见稿》进一步要求，运营者应当对外包开发的系统、软件，接受捐赠的网络产品，在其

上线应用前进行安全检测（第 32 条）；运营者发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当向有关部门报告（第 33 条）。

《征求意见稿》特别指出，关键信息基础设施的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门（第 34 条）。与《网安法》第 37 条要求运营者在境内存储在中华人民共和国境内运营中收集和产生的个人信息和重要数据相比，《征求意见稿》的境内运维要求在数据访问权限的角度更为严格。

四、进一步明确监管工作的开展方式

《征求意见稿》规定，国家网信部门负责统筹协调关键信息基础设施安全保护工作。国家行业主管或监管部门负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。

《征求意见稿》要求监管部门从监测预警、应急预案准备和演练、安全检测评估等多个维度对其行业内关键信息基础设施进行监管。

五、简评

《征求意见稿》在一定程度上对于《网安法》之中关于关键信息基础设施的范围和安全保护措施进行了扩展和细化，但作为行政法规，仍保留了相对的灵活性和解释空间。

对于实践操作而言，在关键信息基础设施的识别、以及具体的各项安全保护措施、采购和报告要求方面，仍有一系列的具体规定需要制定，也将留待后续的标准去进一步规范和实施。

董　潇　　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
袁　琼　　律　师　电话：86 10 8553 7663　邮箱地址：yuanq@junhe.com
周梦瑶　　律　师　电话：86 10 8519 1755　邮箱地址：zhoumy@junhe.com

JUNHE BULLETIN

JUNHE

July 14, 2017

Cybersecurity Law

Draft CII Regulations Released for Public Comment

The Cyberspace Administration of China ("**CAC**") released a draft of *Regulations on Security Protection of Critical Information Infrastructures* (the "**Draft**") on July 11, 2017 allowing for one month of public comment to be offered.

The Cybersecurity Law of the People's Republic of China (the "**CSL**") was first to adopt the concept of critical information infrastructure ("**CII**"). According to Article 31 of the CSL, the concrete scope of CII and security protection rules shall be formulated by the State Council. In *the 2016 Legislative Work Plan of the State Council*, CAC is designated to draft such regulations. The market has long been anticipating the Draft, and expect it to clarify various issues relating to CII, as one of the most critical issues under the CSL. The Draft incorporates comprehensive requirements and regulations in areas like government coordination and precaution mechanism. Below we only summarize those specific areas which are more closely related to companies' compliance obligations.

I. Refining the scope of CII

CII is briefly defined in CSL in Article 31 which provides "the State shall carry out important protection of the important industries and fields, such as public communication and information service, energy, transportation, irrigation, finance, public services and e-government affairs, and the key information infrastructures *that may endanger national security, people's livelihood and the public interest in case of damage, function loss or data leakage* on the basis of classified protection system for network security. The specific scope of CII and security protection measures shall be formulated by the State Council". This definition creates two basic criteria in determining a CII: industrial criteria and consequence criteria.

Article 18 of the Draft further elaborates the criteria of the CSL further and adds certain new industries into the industrial criteria: "the network facilities and information systems operated or managed by the following entities, that may endanger national security, people's livelihood

and public interest in case of damage, function loss or data leakage, shall be included into the scope of CII:

1. Government organs, and entities in the industries or fields of energy, finance, transportation, irrigation, healthcare, education, social security, environment protection, public utilities and so forth;

2. Information networks such as telecommunications networks, radio and television networks, and the Internet; and entities providing *cloud computing, big data, and other public information network services on a large scale*;

3. Scientific research and manufacturing entities in sectors such as national defense and science industry, heavy equipment industry, chemical industry, and food and pharmaceutical industry;

4. News report entities such as radio stations, television stations and news agencies; and

5. Other key entities."

Firstly, the Draft incorporates in the scope of CII industries such as "national defense and science industry, heavy equipment industry, chemistry industry, food and pharmaceutical industry" and etc. which was not enumerated under the CSL.

Secondly, the Draft refines industries such as "public telecommunications and information services", "public services" in the CSL. For example, "public services" is further refined as "healthcare, education, social security, environment protection, public utilities"; "public telecommunications and information services" is refined as entities in "telecommunications networks, radio and television networks, Internet, and entities providing cloud computing, big data, and other public information network services on large scales, radio stations, television stations and news agencies".

According to Article 19 of the Draft, the national cyberspace administration departments, in conjunction with the competent departments for telecommunications and the public security departments, will formulate guidelines for the identification of CII. In practice, although the provisions in the Draft related to the CSL have offered further refinement, the specific scope and standards for determining whether specific facilities would fall into the scope of CII are probably yet subject to identification guidelines to be formulated. The relatively general provisions in the Draft retain to certain extent flexibility for subsequent changes in law enforcement and practice.

II. Reinstating the obligations of CII Operators in Security Protection

Article 31 of the CSL and Article 6 of the Draft both stipulate that the State shall carry out focused protection of CII on the basis of classified protection systems for network security. Operators of CII (the "**Operators**") also belong to network operators, they should therefore at the same time observe the security protection requirements imposed on network operators and the Operators in the CSL.

Chapter IV of the Draft repeats the respective provisions in the CSL, which includes requiring the Operators to:

1. formulate internal security management systems and operating procedures, and strictly enforce identity authentication and authority management;

2. employ technical measures to prevent acts endangering network security, and monitor

and record network operation status;

3. adopt measures such as data classification, backing up important data, and encryption authentication;

4. set up specific network security administration and personnel responsible for network security management;

5. periodically conduct network security education, technical training and skills evaluations for employees;

6. formulate emergency plans for network security incidents and conduct drills regularly;

7. conduct testing and assessment of security of CII at least once per year;

8. store personal information and important data within the territory of China.

Compared to the CSL, the Draft specifies more detailed requirements, such as, the Operators' technical specialist should have obtained certain qualification before taking a position (specific details about the qualification have not been released), education and training for employees should last at least one working day per person each year, and last at least three working days each year for professional technical personnel in key positions, the Operators shall conduct security tests and assessments before CII goes live or when major changes are made.

III. Strengthening the inspecting and reporting obligations for network products and purchase of services

In the aspects of network products and security services, the Draft reinstates a number of requirements in the CSL, which include: network products and services shall meet the mandatory requirements of national law; the purchase of network products or services by operators, which might affect the national security, shall pass the security review and the Operators shall sign a security confidentiality agreement with the provider.

The Draft further requires that Operators shall conduct security testing of systems and software developed by third parties, and of donated network products, before using them online (*Article 32*); Where operators find that network products or services they employ pose risks such as security defects or vulnerabilities, they shall promptly adopt measures to eliminate the threat, and where major risks are involved, they shall report it to the relevant departments in accordance with the provisions (*Article 33*).

The Draft specifically points out that the operation and maintenance of CII shall be carried out within the territory of China. Where it is truly necessary to carry out remote overseas maintenance due to business needs, this should be reported to the state departments for administration or supervision of the industry and the public security department under the State Council (*Article 34*). Compared to Article 37 of the CSL, which states that personal information and important data collected and generated by the Operators during their activities within the territory of the PRC shall be stored within the territory, the requirement of the operation and maintenance of CII in the perspective of data access is more stringent in the Draft.

IV. Further clarification for the performance of regulatory responsibilities

The Draft stipulates that the national cyberspace administration department is responsible for coordinating the protection of CII. The national industry administrative or regulatory departments are responsible for instructing and supervising

the industry's security protection of CII.

The Draft also demands that the supervisory authority should conduct supervision on the CII, ranging from monitoring, warning, taking precautionary steps and drills, to testing and conducting safety assessments and so on.

V. Our Observation

The Draft has expanded and refined on the scope and safety protection measures of the CII in the CSL to certain extent. As an administrative regulation, it remains relatively flexible leaving room for interpretation and enforcement by regulators. We also expect a series of detailed rules and standards are to be formulated to address all the issues related in practice to the identification of CII and the specific details of various aspects in security protection measures, procurement and reporting.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Lena YUAN	Associate	Tel: 86 10 8553 7663	Email:yuanq@junhe.com
Mengyao ZHOU	Associate	Tel: 86 10 8519 1755	Email:zhoumy@junhe.com