君合研究简讯

JUNHE

2017 年 5 月 18 日

电信与互联网法律热点问题

网信办出台首部《网络安全法》实施办法——《网络产品和服务安全审查办法》

国家互联网信息办公室（简称“网信办”）于 2017 年 5 月 2 日正式发布了《网络产品和服务安全审查办法》（试行）（以下简称“《办法》”）。《办法》是《中华人民共和国网络安全法》（以下简称“《网络安全法》”）的首部重要配套实施办法。《办法》将于 2017 年 6 月 1 日与《网络安全法》同时生效。

网信办曾于今年 2 月公布了《办法》草案并进行了为期一个月的公开征求意见。与草案相比，《办法》最终稿并没有重大修改，只是略微缩小了草案规定的审查范围并对审查重点进行了微调，简要介绍如下。

一、法规层级及法律基础

《办法》是以规范性文件而非部门规章的形式发布，这不同于网信办当天发布的另两部规定。[1]《办法》仍为“试行”，以及其以效力层级较低的规范性文件形式发布，可能反映了监管机关对此领域的监管态度是探索性、实验性的。《办法》的上位法依据是《中华人民共和国国家安全法》第五十九条——要求对影响国家安全的网络信息技术产品和服务进行安全审查，及《网络安全法》第三十五条——规定关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

二、需经过审查的产品和服务的范围

某项产品及服务是否需经过国家安全审查有两项判断标准：（1）是否属于重要的产品及服务；以及（2）这些产品及服务是否被用于关系国家安全的网络和信息系统（第二条）。对于什么样的产品及服务会被认定为是“重要的”，以及什么样的信息系统会被认定为是“关系国家安全”， 目前尚无明确规定。最终稿删除了原草案中规定的“关系公共利益”标准。

具体而言，《办法》规定“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，以及其他关键信息基础设施的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，产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定”（第十条）。本条规定基本重复了《网络安全法》的相关规定，赋予了网信办及相关行业主管部门很大自由裁量的空间去决定需进行网络安全审查的产品和服务的具体范围。

三、负责审查的监管部门及主体

[1]与《办法》同天发布的这两部规定是《互联网新闻信息服务管理规定》及《互联网信息内容管理行政执法程序规定》。

安全审查由政府监管机关牵头，结合社会多方参与。

- 网络安全审查委员会

网信办会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。（第五条）

- 网络安全审查办公室

《办法》要求设立网络安全审查办公室负责具体组织实施网络安全审查，但《办法》未明确规定将由哪个机关负责设立该办公室、如何设立。（第五条）

- 网络安全审查专家委员会

网络安全审查委员会将聘请相关专家组成网络安全审查专家委员会，在第三方评价基础上对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估。（第六条）

- 行业主管机关部门

重点行业和领域的主管部门组织开展本行业、本领域网络产品和服务安全审查工作（第八条）。行业主管机关、网信办、及网络安全审查委员会的具体职责划分目前尚不明确，仍有待在实践中观察。

- 第三方审查机构

网络安全审查引入了第三方评价机制，由国家依法认定的网络安全审查第三方机构进行评价（第七条），但《办法》并未明确规定第三方审查机构的资格条件。

四、审查标准

网络安全审查重点审查网络产品和服务的安全性、可控性，主要包括：

（1） 产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；

（2） 产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；

（3） 产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；

（4） 产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险；

（5） 其他可能危害国家安全的风险。（第四条）

《办法》对上述风险的规定都比较笼统，一些具体问题，例如如何对供应链上游，如生产、测试等阶段进行审查，在审查中是否会考虑产品和服务提供者的外资背景，以及什么情形构成损害“用户利益”仍有待在后续实践中明确。

五、持续动态监管

《办法》所规定的网络安全审查是一个多维度、持续的过程。安全审查结合实验室检测、现场检查、在线监测和背景调查等手段，重点对网络产品和服务的安全性、可控性进行审查。网络安全审查办公室可以按照国家有关要求主动启动网络审查程序，也可以根据全国性行业协会建议和用户反映等启动网络安全审查程序。网络安全审查的动态和持续特征体现了近年来政府从事前许可转变为事后监管的趋势，但这种持续的事后监管将如何执行尚有待观察。

六、简评

总体而言，《办法》最终稿仍然比较笼统和抽象，留下了一些有待细化和明确的问题，例如什么样的主体和产品及服务需进行安全审查，新设立的负责审查的机构的组织架构，第三方评价机构的资质，具体的审查程序，以及具体审查标准等。监管机构和标准化委员后续制定的政策和标准可能会对这些问题进一步规定。随着新审查体系的建立，这些问题将逐渐明朗。这些问题的后续发展值得我们密切关注和追踪。

董　潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
蔡克蒙　律　师　电话：86 10 8519 1255　邮箱地址：caikm@junhe.com
郭静荷　律　师　电话：86 10 8553 7947　邮箱地址：guojh@junhe.com

JUNHE BULLETIN

May 18, 2017

Telecommunication Law

CAC Adopted First CSL Ancillary Measures for Network Products and Services Security Review

The Cyberspace Administration of China ("**CAC**") formally adopted *the Measures on Security Review of Network Products and Services (Trial for Implementation)* ("**Measures**") on May 2, 2017, the first and an important ancillary regulation of the Cybersecurity Law ("**CSL**"). The Measures will become effective simultaneously with the Cybersecurity Law on June 1, 2017.

CAC released a draft of the Measures in February of this year allowing for one-month public comment. While the finalized version is not substantially different from the draft, its applicable scope has been narrowed and minor adjustments have been made to the focus of the review, as briefly summarized below.

I. Legal Hierarchy and Legal Basis

Unlike two other regulations issued by CAC on the same day of the Measures[1], the Measures was issued in the form of a normative document (规范性文件) rather than a departmental regulation (部门规章). The title of trial for implementation of the Measures and its lower legal hierarchy may reflect the authority's explorative and experimental attitude towards regulation of the subject matter. The Measures is based on Article 59 of the National Security Law which calls for the establishment of a national security review on network information technology products and services concerning national security, and Article 35 of the CSL which provides that the procurement of network products and services by critical information infrastructure operators must pass a national security review organized by CAC in conjunction with the relevant departments of the State Council.

II. Scope of Products and Services Subject to Review

Two criteria apply to products and services subject to national security review: (a) "important products and services" and (b) "such products and services are used in information system concerning national security" (*Article 2*). Questions remain as to what types of products

[1] The Provisions on Administration of Internet News Information Services and the Provisions on Administrative Enforcement Procedures of Internet Information Content Administration.

and services are considered "important", and what types of information systems are considered "concerning national security" (on this point, "concerning public interest" in the original draft has been removed in the final version).

Specifically speaking, the Measures provides that "the procurement of network products and services by operators in public communication and information services, energy, transportation, hydraulic, finance, public services, e-government and other key industries and sections, and operators of other critical information infrastructure which may affect national security shall pass cybersecurity review," and the relevant critical information infrastructure ("**CII**") protection authority shall determine whether or not certain products and services affect national security. Such a provision reiterates the requirements under the CSL yet offers large discretion to CAC and the relevant industrial regulatory authorities when determining the specific scope of products and services subject to cybersecurity review.

III. Authorities and Entities Responsible for the Review

The security review is steered by regulatory authorities and involves societal participation.

- Cybersecurity Review Committee

  A cybersecurity review committee is to be established by the CAC with other regulatory authorities to review and deliberate major policies relating to cybersecurity reviews, organize cybersecurity review activities and coordinate major issues in this area *(Article 5)*.

- Cybersecurity Review Office

  A cybersecurity review office is to be established to organize and implement cybersecurity review. The Measures does not explicitly provide how the office will be set up *(Article 5)*.

- Cybersecurity Review Experts Committee

  The cybersecurity review committee will engage relevant experts to form a cybersecurity review experts committee who will conduct an overall evaluation on the security risk of network products and services and the security and reliability of their providers on the basis of a third party evaluation *(Article 6)*.

- Industrial Regulatory Authorities

  Industrial regulatory authorities shall organize cybersecurity reviews in key industries and sectors regulated by them *(Article 9)*. However, the specific division of responsibilities between the industrial regulatory authorities, CAC and the cybersecurity review committee remains to be seen in practice.

- Third Party Review Institutions

  The cybersecurity review introduces third party evaluations which are to be carried out by third party review institutions certified by the State *(Article 7)*. The Measures does not yet specify the qualification process for such third party review institutions.

IV. Criteria of Review

The focus of a cybersecurity review is on the security and controllability of network products and services, which largely includes the following risks:

- the security risk contained in the products and services and the relating to them to be illegally controlled, disrupted and interrupted;

- the risk relating to the security of supply chains in the manufacturing, testing, delivering and technical support process of the products and their key components;
- the risk that product and service providers utilize the convenience of providing products and services to illegally collect, store, process and use a user's information;
- the risk that a provider abuses a user's reliance on a product and/or service to endanger the user's interests or cybersecurity; and
- other risks may endanger national security and public interest *(Article 4)*.

The risks listed above are high level points and a number of questions remain such as (a) how to review early stages of the supply chain such as manufacturing and testing, (b) whether foreign shareholding backgrounds of products and services should be considered, and (c) what constitutes "jeopardizing users' interest".

V. Ongoing Supervision

The cybersecurity review under the Measures is a multi-dimensional and ongoing process comprising of a lab-test, an onsite inspection, online monitoring and a background investigation. The cybersecurity review focuses on the security and controllability of network products and services. It may be launched either by the cybersecurity review office in accordance with the relevant national rules or upon the advice of national industrial associations and user feedback. The dynamic nature of the review reflects the general trend of regulatory development moving from ex-ante permit to ex-post supervision. However, the practical implications of ongoing supervision remains to be seen.

VI. Our Observation

In general, the final Measures remain high level and general in nature. The Measures leave a number of outstanding issues such as the specific scope of entities, the products and services subject to the security review, the organization of new authorities to be created in charge of the review, the certification of third party evaluation institutions, and the review procedures and the specific review criteria, which may be specified in policies and standards to be formulated by the relevant authorities and standardization institutions. It is anticipated that a new review system will gradually be introduced to deal with the outstanding issues mentioned above and all these new developments are worthy being followed up.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Kemeng CAI	Associate	Tel: 86 10 8519 1255	Email:caikm@junhe.com
Jinghe GUO	Associate	Tel: 86 10 8553 7947	Email:guojh@junhe.com