JUNHE BULLETIN

JUNHE

June 12, 2019

Cybersecurity Law

MIIT releases draft Implementation Measures on Key Network Equipment Safety Inspection for public comment

On June 5, 2019, the Ministry for Industry and Information Technology ("**MIIT**") released a draft of *Implementation Measures on Key Network Equipment Safety Inspection* (the "**Draft for Comment**"), which will remain open for public comment for one month until July 4.

Article 23 of the *Cybersecurity Law* (the "**CSL**") provides key network equipment and the specialized products for network security which may not be sold or provided until they pass the security certification or security testing conducted by qualified institutions in accordance with the compulsory requirements of the national standards. The national Internet information department shall, in conjunction with relevant departments of the State Council, formulate and promulgate the catalogue of key network equipment and specialized products for network security and promote the mutual recognition of security certification and security testing results to avoid repetitive certification and testing.

The Draft for Comment provides specific requirements on procedures and requirements for security inspection. It refers to 'key network equipment' as those listed in the *Key Network Equipment and Network Security Special Products Catalogue*, according to *Notice on the release of the Key Network Equipment and Network Security Special Products Catalogue (First Batch)* in 2017, which includes routers, switchs, rack servers and programmable logic controllers. MIIT shall be responsible for organizing and carrying out the key network equipment security inspection work (*Article 5*).

The Draft for Comment provides manufacturers of key network equipment which select to conduct security inspection for key network equipment, shall submit application materials (including basic information about the manufacturer and key network equipment, a statement about equipment performance data is in compliance with key network equipment technical parameters, materials relating to the enterprise's security capacity) to MIIT (*Article 6*), then, they shall choose an example product and entrust a qualified institution to conduct security inspection. Such institution will then provide a security inspection report on the selected product to MIIT (*Article 7*). MIIT will publish the list of key network equipment which has passed security inspection with a three year term of validity.

The Draft also provides for any key network equipment subject to telecom device network access permit system, if it has been inspected by

qualified institutions in accordance with the security inspection standard for key network equipment during the process of applying for the network access permit, and it still has a valid network access permit, such key network equipment shall be exempt from repetitive security inspection. The expiration date for such key network equipment will be the expiration date of its network access permit.

The Draft for Comment also provides requirements in respect of information change of key network equipment, obligations and liabilities for manufacturers and inspection institutions and supervision requirements for MIIT.

We will follow up with legislative development of the Draft.

Marissa (Xiao) DONG	Partner	Tel：86 10 8519 1233	Email：dongx@junhe.com
Lena (Qiong) YUAN	Associate	Tel：86 10 8519 2410	Email：yuanq@junhe.com

君合研究简讯

2019 年 6 月 12 日

网络安全法律热点问题

工信部发布网络关键设备安全检测管理办法征求意见

2019 年 6 月 5 日，工业和信息化部（以下简称“**工信部**”）发布《网络关键设备安全检测实施办法（征求意见稿）》（以下简称“**《征求意见稿》**”），向社会公开征求意见一个月至 2019 年 7 月 4 日。

《网络安全法》第 23 条规定，网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

《征求意见稿》对于安全检测方式的程序和要求作出了具体规定。《征求意见稿》所针对的网络关键设备亦指列入《网络关键设备和网络安全专用产品目录》的网络关键设备，根据 2017 年发布的第一批公告，包括路由器、交换机、服务器（机架式）和可编程逻辑控制器。工信部负责组织实施网络关键设备安全检测工作（*第五条*）。

《征求意见稿》规定，网络关键设备的生产企业选择进行网络关键设备安全检测的，应向工信部提交申请材料（包括生产者和网络关键设备的基本信息、设备性能参数符合网络关键设备技术指标的声明、企业安全保证能力相关材料等）（*第六条*）；其次，生产者应选取样品，委托具有资格的机构进行安全检测，经安全检测符合要求后，由检测机构向工信部提交网络关键设备安全检测报告（*第七条*）。工信部将发布通过安全检测的网络关键设备名单，有效期为三年。

《征求意见稿》还提出纳入电信设备进网许可制度管理的网络关键设备，如在进网管理中由具备资格的机构按照网络关键设备安全检测依据的标准实施检测，且进网许可证仍在有效期内的，不再重复检测。有效期届满时间为设备进网许可到期时间。

《征求意见稿》也进一步对于网络关键设备的变更情况说明、生产企业和检测机构的责任和义务、及工信部监督管理等方面做出了规定。

我们将持续跟踪草案的立法进展。

董　潇　合伙人　电话：86 10 8519 1233　邮箱地址：dongx@junhe.com
袁　琼　律　师　电话：86 10 8553 7663　邮箱地址：yuanq@junhe.com