君合研究简讯

JUNHE

2018 年 7 月 13 日

电信与互联网法律热点问题

《网络安全等级保护条例（征求意见稿）》发布

公安部于 2018 年 6 月 27 日发布《网络安全等级保护条例（征求意见稿）》（以下简称**“《征求意见稿》”**），以实施《中华人民共和国网络安全法》（以下简称**“《网安法》”**）第 21 条规定的网络安全等级保护制度。《征求意见稿》颁布后，将更新由《信息安全等级保护管理办法》（2007，以下简称**“《管理办法》”**）建立的信息安全等级保护制度。该《征求意见稿》的主要变化如下：

一、评级标准略有变化

《征求意见稿》中信息系统安全保护等级的五级评级体系与《管理办法》基本保持一致，但“对相关公民、法人和其他组织的合法权益造成特别严重损害的”信息系统对应的保护等级由《管理办法》中规定的第二级提高为第三级标准。

二、《征求意见稿》对第二级信息系统安全保护增加了新规定

除了重申现行法规中的一般安全保护义务外，《征求意见稿》还从以下角度对第二级信息系统的安全保护义务进行了规定：（1）进行专家定级评审；（2）公安机关定级备案；（3）上线运行前进行网络安全测试；（4）每年开展一次网络安全自查和报告安全风险隐患；以及（5）获得行政许可的主体的网络安全等级保护制度落实情况将被相关主管部门纳入审计、审核范围等。

三、《征求意见稿》对第三级及以上信息系统安全保护规定了新义务

三级以上的信息系统的网络安全保护义务与《网安法》中的关键信息基础设施类似。此外，《征求意见稿》还从以下方面规定了新的义务：（1）建设网络安全防护管理平台并与同级公安机关对接；（2）上线前委托网络安全等级测评机构进行等级测评；（3）每年开展一次网络安全等级测评；（4）对网络安全管理负责人和关键岗位人员进行安全背景审查并要求持证上岗等。

四、风险管控的新技术

《征求意见稿》规定，网络运营者有义务采取措施，管控云计算、大数据、人工智能、物联网、工控系统和移动互联网等新技术、新应用带来的安全风险，消除安全隐患。

五、配合政府调查、处置及约谈的义务

《征求意见稿》规定了网络运营者有义务配合、支持公安机关和有关部门开展事件调查和处置工作并采取紧急措施。此外，进一步规定公安部门和其他相关监管机构如发现网络存在较大安全风险隐患或者发生安全事件的，可以约谈网络运营者的法定代表人、主要负责人及其行业主管部门。

六、 涉密网络的密码监管和网络安全保护

《征求意见稿》规定了信息系统使用加密技术的一般义务，并对三级及以上的信息系统的义务进行了更严格的规定。《征求意见稿》还从系统设计、运行维护、日常管理和密码评估等角度对涉密网络密码保护进行了特殊的规定。

七、总结与展望

《征求意见稿》将作为《网安法》的重要配套法规，后续配合多项仍在起草或制定过程中的国家标准实施。各公司将需要加强内部的网络安全和信息保护合规系统和制度建设，以便为即将实行的《征求意见稿》及公安部门的执法工作做好准备。

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

JUNHE BULLETIN

JUNHE

July 13, 2018

Telecommunication Law

Draft Multi-Level Cybersecurity Protection Regulation Released for Public Comment

The draft *Multi-Level Cybersecurity Protection Regulation* **("Draft Regulation")** was released by the Ministry of Public Security **("MPS")** on June 27, 2018 in order to implement the multi-level protection scheme under Article 21 of the *Cybersecurity Law* **("CSL")**. The Draft Regulation provides an update to the original multi-level cybersecurity protection measures addressed in the *Administrative Measures for Multi-Level Protection of Information Security* issued in 2007 **("2007 Measures")**. The key points and changes to the existing requirements arising from the Draft Regulation are as follows.

I. Slight change to the grading criteria

The five-tier system and the criteria for identifying the tiers generally remain the same as in the 2007 Measures. The main difference is that an information system that might cause extraordinarily serious damage to the rights and interests of citizens, legal persons and other organizations, is categorized under the Draft Regulation as Tier 3, whereas they were categorized as Tier 2 under the 2007 Measures.

II. New obligations for information systems of Tier 2 incorporated into Draft Regulation

As well as reiterating the general obligations included in existing laws, the Draft Regulation imposes heightened requirements for Tier 2 information systems, including requiring: (a) expert review for tier identification, (b) filing with the relevant public security authority, (c) testing before putting the information system online, (d) annual self-examination and reporting of security risks, and (e) audit and review of implementation status of multi-level protection system by industrial regulators for licensed businesses.

III. New obligations for Tier 3 or higher level information systems added into Draft Regulation

Similar to the critical information infrastructure requirements under CSL, the Draft Regulation includes obligations relating to cybersecurity for Tier 3 or higher level information systems. The Draft Regulation also sets out new requirements for matters, including: (a) the need to design

cybersecurity prevention and management platforms that can be connected with the relevant public security authority; (b) checking by a testing and evaluation agency before the information system is put online; (c) annual evaluation of the level of security of an information system; and (d) specific requirements for key personnel.

IV. Risk control for new technology

The Draft Regulation generally provides that network operators bear the responsibility to take necessary measures to control the risks associated with new technologies such as cloud computing, big data, artificial intelligence (AI), the internet of things (IOT), industrial control systems and mobile internet.

V. Obligation to cooperate with regulators' inquiries and enforcement

The Draft Regulation restated that requirement in the CSL that network operators are obliged to cooperate and support enforcement by regulators and to take emergency measures as required. In addition, if the relevant public security department and other relevant regulators identify any major security risk, or in the event of any security incident, they may make enquiries of the legal representative or the network operator's main responsible person.

VI. Encryption regulation and cybersecurity protection for information systems involving State secrets

The Draft Regulation outlines various heightened obligations for information systems of Tier 3 or higher in relation to encryption techniques. The Draft Regulation also separately addresses the need for cybersecurity protection for any information system that includes State secrets, including in relation to how the system is built, equipment used and the management, testing and risk assessment associated with products used to protect the secrecy of information.

VII. Our Observation

The Draft Regulation will likely be implemented as a key regulation supporting the CSL, along with several other national standards that are currently still in draft format. We envisage that companies will need to enhance their internal cybersecurity and information protection schemes in order to comply with the Draft Regulation and its enforcement by public security authorities in the near future.

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