LINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16/19 楼
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2592 1978
传真: +852 2868 0883

伦敦
1/F, 3 More London
Riverside, London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

通力法律评述 | 公司及并购
2020 年 4 月

箭已离弦，简评《网络安全审查办法》的影响

作者：杨迅 | 杨坚琪

2020 年 4 月 27 日，网信办对外正式发布了更新版的《网络安全审查办法》。对比 2019 年 5 月发布的《网络安全审查办法(征求意见稿)》，正式生效版的《网络安全审查办法》明显更注重于“网络安全审查制度”的可操作性。《网络安全审查办法》同时也释放出一个积极的信号，在《网络安全法》颁布的四年以后，其中最为重要且最受人瞩目的“关键信息基础设施保护制度”，已经离我们越来越近了。

离弦：《网络安全审查办法》的核心要求

第一，《网络安全审查办法》明确了适用范围。和征求意见稿一致，现行的《网络安全审查办法》限缩了 2017 年颁布的《网络产品和服务安全审查办法(试行)》(“试行办法”)下网络安全审查制度的适用主体。根据《网络安全审查办法》第二条的规定，只有在满足三个条件的情况下，即: 1)采购主体为“关键信息基础设施运营者”; 2)采购的是“网络产品或者服务”; 以及 3)该等采购影响或者可能影响“国家安全的”，关键信息基础设施运营者才需要向有关部门申报网络安全审查。

第二，关键信息基础设施运营者应当在申报前进行“风险”预判，以评估相关的风险是否需要进行网络安全审查。根据《网络安全审查办法》第 5 条的要求，关键信息基础设施运营者应当参照关键信息基础设施保护工作部门为各行业制定的预判指南，以进行相应的“风险”预判工作。一般而言，需要考虑的因素包括:

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

- 产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险;
- 产品和服务供应中断对关键信息基础设施业务连续性的危害;
- 产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险;
- 产品和服务提供者遵守中国法律、行政法规、部门规章情况;
- 其他可能危害关键信息基础设施安全和国家安全的因素。

考虑到本次《网络安全审查办法》是由网信办牵头，公安部、工信部、央行等 12 个政府部门共同发布的，可以预见的是各行业各领域的“预判指南”将由各个主管部门陆续颁布，以推进相关工作的开展。

第三，《网络安全审查办法》完善了“网络安全审查制度”的制度设计，保障“网络审查制度”得以落实。2017 年的《网络产品和服务安全审查办法(试行)》颁布后，“网络安全审查办公室”在执法实践中的作用尚不明显，加之“关键信息基础”的认定方法也尚未出台，因此试行办法未能真正地发挥作用。本次《网络安全审查办法》的官方解读明确说明具体的审查工作将由“中国网络安全审查技术与认证中心”(原中国信息安全认证中心)承担。这样的制度安排至少解决了“审查端”的权责问题，也意味着一旦未来“关键信息基础设施”的认定工作启动，那么网络安全审查制度就能够得以顺利实施。

最后，《网络安全审查办法》还针对采购活动相关的合同内容提出了要求。在征求意见稿中，主管部门就已经要求关键信息基础设施运营者必须通过合同的方式约束网络产品或服务的提供者配合网络安全审查。而此次正式稿则进一步提出，双方签订的采购合同中应当包括“网络安全保证”、“业务连续性保证”等条款。值得一提的是，正式稿删除了曾在征求意见稿中出现的“产品和服务提供者约定网络安全审查通过后合同方可生效”的要求；但是根据官方公布的指导意见，关键信息设施运营者仍然被建议应当在合同签署前即进行网络安全审查的申报，如果一定要在合同签署后申报网络安全审查的，那么仍然应当在合同中保留合同生效要件的限制。

此外，虽然更新版的《网络安全审查办法》将在 6 月 1 日正式生效，但部分敏感行业的主管机关似乎已经开展大规模的排摸检查活动。这可能是对本行业网络安全状况的摸底，为将来出台更加贴切的执法指引做准备。

中靶：《网络安全审查办法》的待决问题

虽然《网络安全审查办法》已经颁布，但是不可回避的一个事实是，如果没有其他配套法律的进一步配合，《网络安全审查办法》可能仍然面临实践中的“无法执行”的困难。

首先，限制《网络安全审查办法》的第一个因素，就是“关键信息基础设施”的范围不明确。作为“网络安全法”的重要支持制度，“关键信息基础设施”的认定范围或认定方法至今仍然未能出台。虽然主管部门零散地发布了一些指导性文件，例如《关于关键信息基础设施安全保护工作有关事项的通知》(网信委【2019】3 号)、《关于开展关键信息基础设施安全保护工作的指导意见》(公网安【2019】917)，或者针对关键信息基

础设施运营者召开了一些非公开会议(例如各省市的年度网络安全工作会议)，但是这些都不足以成为认定“关键信息设施运营者”的合法因素或依据。

第二，是“国家安全”的界定问题。无论是《国家安全法》，还是《网络安全法》，都没有对于“国家安全”给出一条具体的判断路径。无论是对于采购的基础设施运营者而言，还是对于网络产品和服务的供应商而言，他们在进行“预判”时都没有足够的依据进行分析。这可能会产生两难境地：即为了保证采购的合法性，无论是否影响“国家安全”，都向有关部门申报网络安全审查，最终使得审核机关不堪重负；或者相反地，为了减轻义务，尽量不选择申报安全审查，最终导致网络安全审查制度“流于形式”。无论是哪一种局面，我们相信这都并非是主管部门的预期。

最后，则是商业秘密的问题。虽然《网络安全审查办法》一再强调审核人员应当负有保密义务，但是仅仅是保密承诺和文字上的保密义务，并不能完全保证商业秘密不被不当披露或者不法使用。尤其考虑到负责网络安全审查的是“中国网络安全审查技术与认证中心”这样一个具有官方背景的机构，其保护网络运营者商业秘密的意愿和能力，难免会引起网络运营者，尤其是外国投资的网络运营者的疑虑。

弓手：在《网络安全审查办法》生效前的准备

关键信息基础设施运营者进行网络安全审查的义务，已是“离弦之箭”。对于可能被认定为关键信息基础设施运营者的单位或者机构而言，为了更好地履行网络安全审查制度的要求，我们建议提前准备如下工作：

- 根据《网络安全审查办法》的要求，针对拟进行的采购进行自我评估；
- 修订相关的采购合同，以保证其符合《网络安全审查办法》的规定，同时确保该些合同中包含关于“服务和产品提供商支持配合审查”、“同意披露有关技术信息”等条款；
- 对于需要提交“中国网络安全审查技术与认证中心”审查的文件，就“必须提交”、“可以提交”和“不必提交”的内容进行研判，从商业秘密保护角度确定提交审查的内容；
- 开展相关的培训，以保证业务部门在实施采购前，了解法律法规的要求。

考虑到《网络安全审查办法》的一切问题仍然需要回归到“关键信息基础设施运营者”的认定这一核心问题上来，这也意味着一拖再拖的关键信息基础设施的认定规则也将是箭在弦上，不得不发了。

如您希望就相关问题进一步交流，请联系：

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	香港	伦敦
T: +86 21 3135 8666 F: +86 21 3135 8600	T: +86 10 8519 2266 F: +86 10 8519 2929	T: +852 2592 1978 F: +852 2868 0883	T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野