

《关键信息基础设施安全保护条例》与企业上市合规

作者：潘永建 | 邓梓珊 | 胡鑫超

2021 年 7 月 30 日，国务院正式公布《关键信息基础设施安全保护条例》(以下简称“《条例》”), 自 2021 年 9 月 1 日起施行。为介绍《条例》有关情况，国务院新闻办公室于 2021 年 8 月 24 日举行国务院政策例行吹风会，我们注意到，吹风会所传递的信息引起了社会各界的重点关注。会上，有媒体记者就《条例》对企业境外上市计划有何影响进行提问，国家互联网信息办公室领导对此表示：

“《条例》并不是针对外贸以及境外上市而出台的，《条例》是围绕保障关键信息基础设施安全，维护网络安全。长期以来，我们积极支持网信企业依法依规融资发展。无论是哪种类型的企业，无论在哪里上市，两条是必须符合的：一是必须符合国家的法律法规。二是必须确保国家的网络安全、关键信息基础设施的安全、个人信息保护的安全等。符合这两条就不受影响，不符合这两条就一定会受影响。”

吹风会过后，各行业拟上市企业，尤其是拟赴境外上市的企业可能形成一种较为“片面”的认知，认为监管部门在《条例》生效之后，可能以“影响国家安全”为由，给相关企业上市增设门槛。由于此前“滴滴出行”等企业因涉及“境外上市”“关键信息基础设施”“网络安全审查”导致业务受影响，此次监管部门释放的“信号”更是引发了担忧。其实，早在《条例》公布之前，监管部门和上市审核机关已经提高了对企业网络安全和数据合规的关注。为帮助上市企业与拟上市企业厘清合规义务，我们通过本文对关键信息基础设施运营者(CIO)和一般运营者在企业上市场景下的网络安全和数据合规风险进行梳理和分析。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

一. CIIO 的网络安全审查义务

根据《条例》，关键信息基础设施是指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、国防科技工业等重要行业和领域的，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、公共利益的重要网络设施、信息系统等。实际上，CIIO 将由保护工作部门(即相关重要行业、领域的主管部门和监督管理部门)根据其制定的认定规则认定并通知。

企业一旦被认定为 CIIO，应履行相应的法定义务(具体各项义务请参见通力法评[《<关键信息基础设施安全保护条例> 企业合规速览》](#))，其中与企业上市最为相关的即是网络安全审查。具体而言，当 CIIO 采购核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务，应预判产品和服务投入使用后的国家安全风险，如影响或可能影响国家安全，应申报网络安全审查。如 CIIO 未自行申报，网络安全审查工作机制成员单位认为影响或可能影响国家安全，仍可能依职权启动网络安全审查，届时则可能面临上市进程受影响的情况。

二. 一般网络运营者的网络安全审查义务

按照《条例》第 20 条和《网络安全审查办法》的规定，如一般网络运营者为 CIIO 提供服务，则仍需配合 CIIO 履行网络安全审查义务，与 CIIO 签订安全保密协议，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。

此外，根据最新的《网络安全审查办法(修订草案征求意见稿)》，除 CIIO 采购网络产品和服务的情形外，掌握超过 100 万用户个人信息的运营者赴国外上市也可能成为网络安全审查的触发条件，此处所指的“上市”包括境内公司在国外的 IPO(首次公开募股)、SPAC(特殊目的收购公司上市)、RTO(反向收购上市)、Direct Listing(直接上市)，以及已上市公司的增发和发债等。值得注意的是，由于此项表述为“国外上市”，赴香港上市的企业“被国外政府影响、控制、恶意利用的风险”的可能性相对较小，故赴香港上市的企业通常不会因上市触发网络安全审查，但不排除因其他因素而受到网络安全审查的可能。

即使企业已在国外上市，例如“滴滴出行”“运满满”“货车帮”“BOSS 直聘”等，网络安全审查办公室仍以网络产品和服务、数据处理活动、国外上市等行为影响或可能影响国家安全为由发起网络安全审查，故不论是否被认定为 CIIO，已上市企业均存在受到网络安全审查的风险。

三. 总体网络安全与数据合规义务

对于拟在国内上市的企业而言，虽然其上市行为受到网络安全审查的可能性较低，但其网络安全与数据合规情况仍会受到上市审核机关的关注。从过往案例来看，从数据堂因员工涉嫌刑事犯罪被暂停股票转让，到墨迹天气因违规收集个人信息上市申请被否，网络安全与数据合规问题逐渐落入上

市审核机关的“射程”范围内。根据公开资料统计, 2020 年共有至少 32 家拟上市企业在上市过程中收到发审委有关网络安全与数据合规方面的问询, 网络安全与数据合规显然已经成为企业上市的核心要素。

根据我们的观察, 上市审核机关主要关注以下几方面内容:

- (1) 网安数据政策变化、行业监管规定对业务持续性的影响;
- (2) 网络与信息系统等保情况、安全技术措施和实施效果等;
- (3) 数据内控制度完备性和有效性;
- (4) 数据来源、数据应用的总体合法合规性;
- (5) 业务过程中收集使用的个人信息类型、来源合法性、全流程使用合规等。

此外, 有关网络安全与数据合规的违法行为不仅可能成为企业上市阶段的拦路虎, 上市后仍可能受到相关监管。例如, 杭州顺网科技股份有限公司曾因数家子公司违法收集用户个人信息受到 130 万元的罚款处罚, 进而引来深圳证券交易所发送的问询函。

总结而言, 网络安全审查制度并非一项全新的制度, CIO 运营者需履行的义务也早在《网络安全法》等法律法规中有所明确。近期的网络安全审查案例和《条例》的施行仅是将相关制度予以具体落实和细化, 而并非专门针对企业的境外上市行为。鉴于上市审核机关针对拟上市企业的问询技术性强、覆盖面广、紧贴相关法律法规要求, 所有拟上市企业均应严格履行《网络安全法》《数据安全法》《个人信息保护法》等法律法规下的网络安全与数据合规义务。

如您希望就相关问题进一步交流，请联系：



潘永建
+86 21 3135 8701
david.pan@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

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

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

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +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



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2021