面对《网络安全审查办法》修订，已/拟国外上市公司如何自我审视？

2021年7月10日，国家互联网信息办公室（以下简称“网信办”）发布《网络安全审查办法（修订草案征求意见稿）》（以下简称“《修订草案》”）。一方面，《修订草案》扩张了网络安全审查的适用范围，从关键信息基础设施运营者（以下简称“**CIIO**”）的采购活动与供应链安全，扩张至同时包含一般数据处理者在数据处理活动中的数据安全；另一方面，《修订草案》继续以“国家安全”为落脚点，网络安全审查的适用门槛仍限于“影响或者可能影响国家安全”的情形。国外上市成为引发审查的重要关注点。

本文聚焦于已国外上市公司、拟国外上市公司（以下合称“已/拟国外上市公司”）的视角，重点评析在《网络安全审查办法》修订的大背景下，已/拟国外上市公司如何有针对性地进行自我审视与合规应对。

一、《网络安全审查办法》修订背景：强化跨境数据安全管理的监管环境

近期，我国监管机构在网络安全、数据保护、证券合规等领域的立法与执法行动频发，呈现出强监管态势。网络安全审查制度作为监管网络中的节点之一，与其他机制环环相扣、相辅相成。

1. 《修订草案》为《数据安全法》下的数据安全审查提供细化规定

《国家安全法》第59条建立了国家安全审查制度，对影响或可能影响国家安全的网络信息技术产品和服务进行国家安全审查；《数据安全法》第24条建立了数据安全审查制度，对影响或可能影响国家安全的数据处理活动进行国家安全审查。

但是，《数据安全法》并未对数据安全审查进行具体规定，目前也缺乏可供参考的实施细则。在《数据安全法》即将于9月1日生效前的窗口期，《修订草案》特别将数据处理活动（尤其针对核心数据、重要数据和大量个人信息）纳入网络安全审查的范围，并在第10条简要提出了数据相关的审查因素，为数据安全审查制度提供了指引性的规定。

具体而言，《修订草案》在坚持“影响或者可能影响国家安全”大原则的同时，将网络安全审查的适用范围扩张至数据处理者开展的数据处理活动。一般的数据处理活动或许难以上升至国家安全层面，但国外上市在上市申请中和上市后均难以避免向国外监管机构提供材料，数据安全风险亦将提升。

《修订草案》的网络安全审查覆盖了国外上市的事前事后全流程，为数据安全与证券监管预留了充分的空间。对于拟国外上市公司，《修订草案》为“掌握超过100万用户个人信息的运营者”设定了主动申报的义务；即使不满足100万的标准，或已国外上市公司，仍然可能被依职权提起审查，其关注重点在于核心数据、重要数据、大量个人信息的窃取、泄露、毁损，和“非法”利用、出境，以及国外政府对上述数据的影响、控制、恶意利用。

2. 《修订草案》与跨境证券监管形成支撑与呼应

2021年7月6日，中共中央办公厅、国务院办公厅印发《关于依法从严打击证券违法活动的意见》，要求完善数据安全、跨境数据流动、涉密信息管理等相关法律法规，尤其在境外发行证券与上市中压实境外上市公司信息安全主体责任。一方面，加强跨境监管合作；另一方面，对抗境外机构对中概股公司的信息披露要求（如美国《外国公司问责法案》）。

在加强跨境证券监管的大背景下，《修订草案》专门在国家网络安全审查工作机制中加入中国证券监督管理委员会，并就国外上市行为进行特别规定，从而为已/拟国外上市公司的监管创设了网络安全审查的防线。目前，已有若干公司取消或搁置了其赴国外上市的计划，更多拟国外上市公司正在观望监管态度、并适时作出相应调整。

二、已/拟国外上市公司如何解读《修订草案》的重点变化

1. **“掌握”和“不掌握”个人信息的界限何在？**

根据《修订草案》第6条，掌握超过100万用户个人信息的运营者赴国外上市，必须申报网络安全审查。在我国当前的互联网发展规模下，100万用户个人信息是一个较低的门槛。拟国外上市公司在实践中采用业务剥离、数据托管等模式有助于降低因上市而导致数据被国外政府调取的风险，但能否因此被认为“不掌握”个人信息尚不清晰。

1. 拟国外上市公司将个人信息相关业务剥离至非上市的关联公司，由关联公司开展个人信息处理活动。这一模式在一定程度上可以避免拟国外上市公司直接掌握个人信息、进而消减国外监管机构获取相关数据的可能性。

2. 拟国外上市公司将个人信息交由非关联的第三方托管，其仅在依据托管协议及用户单独授权的情况下才可处理个人信息。例如，微软在德国运营云计算服务Azure时，将数据的控制权交由德国的数据托管机构，微软无法自行访问数据。拟国外上市公司可以申明已通过协议让渡对数据的控制权，但合同约定具有相对性，实践中可能难以彻底对抗监管要求。

2. 不掌握个人信息就无需顾忌网络安全审查吗？

对于赴国外上市前必须申报网络安全审查的适用范围，《修订草案》第6条仅规定了“掌握超过100万用户个人信息”的情形，但从全文来看，国外上市可能影响国家安全时，也可能引发依职权启动的网络安全审查。

1. 重要数据与核心数据。《修订草案》在立法依据中新增了《数据安全法》，而重要数据和核心数据正是《数据安全法》的重点之一，且在《修订草案》第10条中和“大量个人信息”并列，同样作为网络安全审查的考虑因素。目前，我国关于重要数据和核心数据的目录还不明晰，但已有立法征求意见稿开始尝试界定重要数据，企业应当对此予以充分重视。

2. 依职权审查。除主动申报之外，《修订草案》第16条规定了依职权审查的模式，网络安全审查工作机制成员单位认为数据处理活动、国外上市行为影响或可能影响国家安全的，经报批程序后可启动审查。当前正是数据合规监管的敏感时期，不排除监管机构开展普查

摸底活动，但从《修订草案》第10条而言，监管本意是针对“核心数据、重要数据、大量个人信息”的“窃取、泄露、毁损以及非法利用或出境”，而非任何数据的任何处理活动都一概纳入网络安全审查。

3. 已国外上市公司可以独善其身吗？

《修订草案》新增的第6条直接针对拟国外上市公司，但从实质而言，网络安全审查的关注点在于国外上市对我国国家安全、数据安全的影响，这既包括上市前的预防性审查，也包括上市后的监督性审查。《修订草案》第10.6条矛头直指国外上市后我国数据“被国外政府影响、控制、恶意利用的风险”，因此，已国外上市公司虽然不必补充申报，但仍然可能被依职权提起审查。

在某种程度上，已国外上市公司具有更强的审查必要性。在上市申请中，拟国外上市公司可能对外提供的主要是与上市相关的数据，有关的国外监管机构一般仅限于证券监管机构（如美国SEC）。在上市后，已国外上市公司受制于更多的国外监管机构，涉及的数据范围可能更广。例如，外国公司在美上市后将会受到FCPA的管辖，FCPA调查往往需要公司披露经营活动中的大量文件、可能涉及公司的核心业务数据。除了SEC外，DOJ也可以启动FCPA调查。结合《数据安全法》第36条，公司向外国司法或执法机构提供境内数据的，须经主管机关批准，由此可能触发网络安全审查。

4. 国外上市行为动辄得咎？

《修订草案》在近期数据合规事件高潮迭起的大环境中发布，进一步加剧了市场的紧张情绪，不免引发过度解读的倾向。在修订前，网络安全审查的适用范围仅限于“CIIO”在“采购网络产品和服务”中“影响或者可能影响国家安全”的情形；在修订后，其适用范围扩张至一般数据处理者的数据处理活动、国外上市行为，因此引发了广泛关注。

事实上，网络安全审查仍然落脚于“影响或者可能影响国家安全”的情形，并非所有的数据处理活动、国外上市行为一概而论。根据《修订草案》第10条，从客体上，网络安全审查聚焦于核心数据、重要数据、大量个人信息（如第6条的“100万”）；从后果上，网络安全审查聚焦于对上述数据的窃取、泄露、毁损、“非法”的利用、出境，以及国外政府对上述数据的影响、控制、恶意利用。

以数据出境为例，并非数据一概不能出境，数据仍然可以“依法”出境。根据《数据安全法》第31条，CIIO的重要数据出境适用《网络安全法》的规定、其他数据处理者的重要数据出境适用网信办的规定，个人信息的出境则依据将来《个人信息保护法》的规定。

三、已/拟国外上市公司应对网络安全审查的合规建议

近期，我国监管机构在网络安全、数据保护、证券合规等领域的立法与执法行动频发，《数据安全法》即将在9月1日正式施行。在这个敏感时期，《网络安全审查办法》发生修订，且修订内容高度匹配近期的监管重点，《修订草案》有可能在短期内生效。

面对《修订草案》，我们对已/拟国外上市公司提出以下合规建议：

1. 对公司数据资产进行全面盘查，按照数据分类分级的思路，梳理个人信

息、重要数据、核心数据的类型、数量、处理目的与方式。

2. 对公司业务进行全面检视，梳理可能存在的数据风险及风险等级，尤其是其中影响或可能影响国家安全的情形。

3. 掌握超过100万用户个人信息的拟国外上市公司，依法申报网络安全审查，并为审查预留充分的时间（如至少留出半年时间），同时做好业务受影响（如暂停注册新用户）的准备。即使采取个人信息业务剥离、数据托管等模式，亦需充分评估监管机构对以该等模式实现风险规避的接受度。

4. 对于数据出境活动，事前开展必要性与风险评估；对于外国司法或执法机构要求提供境内数据的情形，提供前主动报主管机关批准；对于已经出境的数据，及时复盘并视情况采取补救措施。

5. 持续跟进立法与执法动向，与监管机构保持良好沟通。

6. 持续加强公司内部的数据合规体系建设，提升数据治理整体水平。