HANKUN
汉坤律师事务所
Han Kun Law Offices

汉坤专递

2021 年第 7 期（总第 171 期）

新法评述

1、《网络安全审查办法》（修订草案征求意见稿）快评

2、《网络产品安全漏洞管理规定》简评

新法评述

1、《网络安全审查办法》（修订草案征求意见稿）快评

作者：段志超丨周颖丨蔡克蒙

中共中央网络安全和信息化委员会办公室，暨中华人民共和国国家互联网信息办公室（简称**“网信办”**）于 2021 年 7 月 10 日颁布了《网络安全审查办法》（**“《审查办法》”**）（修订草案征求意见稿）（**“征求意见稿”**），明确了数据处理者（以下称**“运营者”**）开展数据处理活动，包括赴国外上市，影响或可能影响国家安全的，将纳入网络安全审查范围。本文将对征求意见稿进行初步解读，并分析其潜在影响。

一、修订要点概述

（一）审查范围扩大至包括特定数据处理者赴国外上市

根据《网络安全法》和征求意见稿，网络安全审查制度审查的重点对象是关键信息基础设施运营者（**“CIIO”**）采购网络产品和服务（《审查办法》第 2 条），但同时相关监管部门具有依职权将其认为有可能影响国家安全的网络产品和服务纳入审查（《审查办法》第 15 条）。在《审查办法》基础上，征求意见稿明确将数据处理者（**“运营者”**）开展数据处理活动，影响或可能影响国家安全的，纳入了网络安全审查范围（征求意见稿第 2 条）。

（二）明确了掌握 100 万用户个人信息的运营者赴国外上市的强制网络安全审查申报义务

征求意见稿规定**“掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。”**因此，即使不属于 CIIO，如果处理用户个人信息数量超过特定量级，其在赴国外上市前亦必须申报网络安全审查。为应对新增的审查范围，征求意见稿明确将证监会纳入中央网络安全和信息化委员会领导网络安全审查工作机制的范畴，与此前的网信办等十二部委联合开展审查。就该规定，如何认定用户数量标准亦存在一定疑问，例如 100 万用户是否仅指境内用户，还是亦包括境外用户，相关标准有待进一步明晰。

（三）审查要点和标准从网络安全扩展至数据安全

传统上《审查办法》主要针对 CIIO 采购特定网络产品和服务相关的供应链安全风险，而征求意见稿明确将《数据安全法》补充为立法依据，且将审查范围扩展至 CIIO、数据处理者数据处理活动以及赴国外上市相关的国家安全风险，特别是“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险；国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险”。需注意的是，“核心数据”[1]和“重要数据”[2]均系近期出台并将于

[1] 《数据安全法》第 21 条：关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

[2] 《数据安全法》第 21 条：国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护……各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

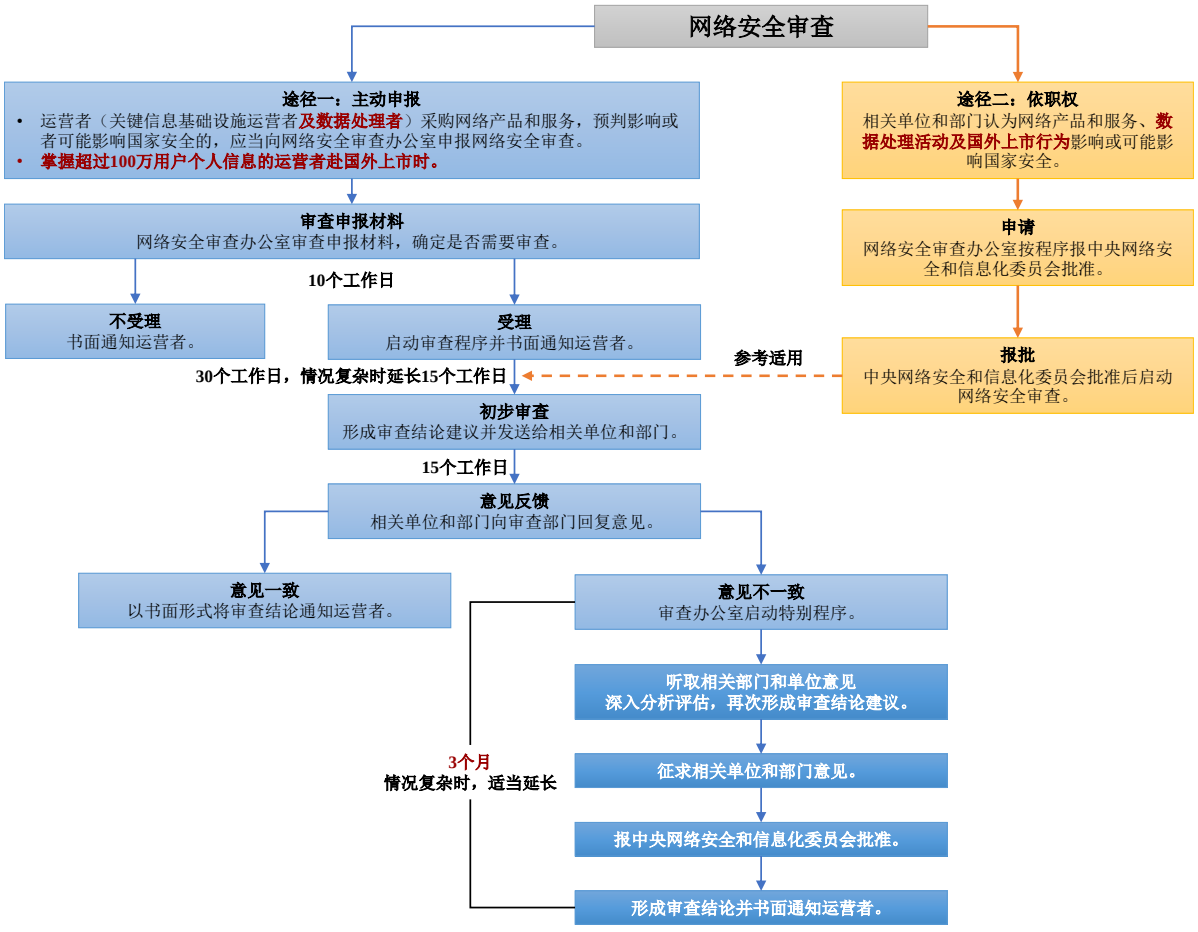
9 月 1 日正式实施的《数据安全法》提出的重要概念，目前均未界定其具体范畴。

（四）申报材料及审查流程相应变更

总体而言，《审查办法》确定的审查材料和审查流程变化不大，但对于赴国外上市的情况而言，需要将“拟提交的 IPO 材料等”提交审查，鉴于赴境外上市所需提交的材料众多，具体需要提交的范围及审查重点仍有待在实践中进一步明确。

根据此前《审查办法》出台时网信办的答记者问，网络安全审查工作具体委托中国网络安全审查技术与认证中心承担，中心在网络安全审查办公室指导下，承担接受材料、对申报材料进行形式审核、具体组织审查工作等任务。

征求意见稿的审查流程总体沿用了现行审查办法的流程，只是将在出现网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门意见不一致情况下，需征求有关部门意见并报中央网络安全和信息化委员会批准的特别审查流程期限由 45 个工作日延长至 3 个月，且情况复杂的仍可以延长。按照征求意见稿，审查流程总体如下图所示。



二、对中概股公司国外上市的影响

（一）“赴国外上市”是否包括香港上市

值得注意的是，征求意见稿使用的是“国外上市”的概念，而非此前法规政策，特别是《证券法》及其配套法规以及数据安全相关法律法规所常用的“境内”和“境外”的概念。如《证券法》第 2 条规

定“在中华人民共和国境内，股票、公司债券、存托凭证和国务院依法认定的其他证券的发行和交易，适用本法”，第 224 条规定“境内企业直接或者间接到境外发行证券或者将其证券在境外上市交易，应当符合国务院的有关规定”。《网络安全法》第 37 条规定“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定”。因此单就文意而言，征求意见稿似乎有意用了“国外上市”的概念，而非其他证券相关法规中包括了香港上市的“境外上市”的概念，这表明赴香港上市可能并不在网络安全审查范围之内。但鉴于征求意见稿并未对此有明确解释，其最终含义仍有待相关监管机构后续在《审查办法》终稿或实践中加以明确。

（二）“赴国外上市”是否包括 SPAC、RTO、Direct Listing 等

除 IPO（首次公开募集股份并上市）外，中概股公司在美国上市还可以采取 SPAC（特殊目的收购公司）并购、RTO（反向兼并/借壳上市）、Direct Listing（直接上市）等方式。虽然征求意见稿在要求企业提交的审查材料中与上市相关的材料仅明确提到“拟提交的 **IPO 材料**”，但鉴于无论哪种上市模式，中概股公司都需要在上市过程中公开披露或向国外交易所及证券监督机构提供信息，并在上市后持续定期披露相关信息，接受国外交易所及证券监督机构的监督和调查，这些都与 IPO 同样可能存在征求意见稿提到的网络安全审查将重点评估的国外上市可能带来的国家安全风险因素，包括“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险”、“国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险”。因此我们认为无论以何种方式在美国或者其他国外交易所完成上市，都可能落入网络安全审查的范围内。

（三）“赴国外上市”是否包括香港二次上市

如果如前述第（一）条分析，国外上市不包括香港上市，则香港二次上市应该也不会包括在在网络安全审查的范围内。但如果《审查办法》最终规定香港上市需要进行网络安全审查，我们认为香港二次上市可能也会包括在审查范围内。这是因为于中概股公司在进行香港二次上市时及上市后可能需要根据香港上市规则额外披露或提供信息，并且也将受限于香港联交所及证券监督机构的监督和调查，因此对于已经通过网络安全审查或者已经在《审查办法》生效前在境外上市的中概股公司而言，香港二次上市也存在增加数据安全风险的可能性。

（四）对已在国外上市的中概股公司增发和发债的影响

征求意见稿并未明确规定已经在国外上市的中概股公司的增发及发债是否属于网络安全审查的范围。我们倾向于认为增发及发债，特别是在上市阶段已经通过网络安全审查的中概股公司的增发和发债，可能不会包括在需要审查的范围内。首先，征求意见稿规定需要进行审查的是“掌握超过 100 万用户个人信息的运营者赴国外上市”，而非证券发行或上市。其次，对于已经在国外上市的中概股公司而言，是否进行增发和发债不会影响其需要遵守的信息披露规则及接受的境外交易所和证券监督管理机构的监督和调查，因此企业在这些方面的数据安全风险不会实质增加。但鉴于中概股公司进行增发和发债可能会在年报、季报等定期披露的信息以外额外披露财务信息，也不能排除监管认为存在数据安全风险增加的风险。因此是否会将已上市的中概股公司的增发和发债包括在审查范围内，包括是否会区分对待已经就上市通过网络安全审查的中概股公司和未进行过安全审查的中概股公司（包括在《审查办法》生效前已经上市的、或者在上市时未达到审查条件的企业），仍有待相关监管机构后续在《审查办法》终稿或实践中加以明确。

（五）对已在国外上市的中概股公司是否有溯及性影响

征求意见稿未明确要求《审查办法》生效时已经在国外上市的中概股公司申报网络安全审查。但征求意见稿第 16 条规定“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的网络产品和服务、数据处理活动以及国外上市行为，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查”。根据该条规定，监管部门有权对已经上市的中概股公司的日常数据处理活动进行安全审查，并在审查中考虑到其国外上市状态。对于国外上市（及上市后增发、发债等）的事前网络安全审查而言，如果出现最终未通过的情况，其后果会比较明确，即企业不能进行上市、增发、发债。但如果监管部门对已经上市的中概股公司进行审查，则最终未通过审查的企业将如何处理将有待法规和监管的明确。

三、建议

对于处理大量个人信息或敏感信息的企业，特别是拟赴或已在境外上市此类企业，为提高企业顺利通过网络安全审查的成功率，我们建议企业：

- 紧跟监管机构对个人信息保护的动态，避免收集与服务无关的个人信息，特别是敏感个人信息，不断完善用户信息保护工作。
- 密切关注监管机构后续出台的重要数据认定标准，全面贯彻落实重要数据保护、安全风险评估、数据本地化等系列要求。系统建立数据安全影响评估制度、内部合规治理制度，对高风险数据处理活动开展事先评估，并持续开展数据合规审计工作。
- 进一步完善网络产品和服务的供应链安全审查，通过事先供应商合规评估、协议约束、事中事后审计等方式，防范采购的网络产品和服务导致运营者系统被非法控制、干扰，数据被泄露、窃取或毁损的风险，确保其供应链安全、开放、透明、来源多样、可持续，不会受到非法控制、干扰，并可有效防范数据泄露、窃取或毁损。
- 在向境外交易所和监管机构提供数据前，按照《数据安全法》第 36 条及《证券法》第 177 条等法律法规的规定事先征求网信办、证监会等主管部门意见，并制定内部制度明确前述要求。
- 密切关注后续配套审查标准的出台和落地。

2、《网络产品安全漏洞管理规定》简评

作者：段志超丨解石坡

2021 年 7 月 12 日，工业和信息化部（“**工信部**”）、国家互联网信息办公室（“**网信办**”）和公安部联合发布了《网络产品安全漏洞管理规定》（“**《漏洞管理规定》**”），自 2021 年 9 月 1 日起施行，为网络安全监管这一近期备受关注的领域再添新规。

根据《漏洞管理规定》，网信办将负责统筹协调网络产品安全漏洞管理工作，工信部负责网络产品安全漏洞综合管理，并承担电信和互联网行业网络产品安全漏洞监督管理，而公安部负责网络产品安全漏洞监督管理，依法打击利用网络产品安全漏洞实施的违法犯罪活动。

《漏洞管理规定》适用于网络产品（包括硬件和软件产品）提供者，网络运营者，从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人，规定了这三类主体的法律义务和违法后果。同时，其要求其他组织或个人不得利用网络产品安全漏洞从事危害网络安全的活动，不得非法收集、出售、发布网络产品安全漏洞信息，并且不得为利用网络产品安全漏洞从事危害网络安全的活动的主体提供技术支持、广告推广、支付结算等帮助。

鉴于网信办近日颁布了《网络安全审查办法》（修订草案征求意见稿）,其中强调了网络安全审查申报制度（汉坤此前的分析请见本专递上一篇*《网络安全审查办法》（修订草案征求意见稿）快评*）对数据处理活动相关的数据泄露、窃取、毁损的风险的考量，《漏洞管理规定》的相关规定将对相关企业针对网络安全审查进行内部自查和对标具有较强的参考作用。

下表是本所对《漏洞管理规定》对于不同适用主体的有关规定的总结：

适用主体	鼓励事项	法律义务	违法后果
网络产品提供者	建立所提供网络产品安全漏洞奖励机制，对发现并通报所提供网络产品安全漏洞的组织或者个人给予奖励。	■ 建立健全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于 6 个月； ■ 发现或者获知所提供网络产品存在安全漏洞后，应当立即组织验证，评估危害程度和影响范围，及时组织修补漏洞； ■ 在 2 日内向工信部网络安全威胁和漏洞信息共享平台报送相关漏洞信息； ■ 对属于其上游产品或者组件存在的安全漏洞，应当立即通知相关产品提供者； ■ 对于需要产品用户（含下游厂商）采取软件、固件升级等措施的，应当及时告知漏洞风险及修	■ 责令改正，给予警告； ■ 拒不改正或者导致危害网络安全等后果的，处 5-50 万元罚款； ■ 对直接负责的主管人员处 1-10 万元罚款。

适用主体	鼓励事项	法律义务	违法后果
		补方式，并提供技术支持。	
网络运营者		■ 建立健全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于 6 个月； ■ 发现或者获知其网络、信息系统及其设备存在安全漏洞后，应当立即采取措施，及时进行验证并完成修补。	一般网络运营者： ■ 责令改正，给予警告； ■ 拒不改正或者导致危害网络安全等后果的，处 1-10 万元罚款； ■ 对直接负责的主管人员处 5,000 元-5 万元罚款； 关键信息基础设施的运营者： ■ 责令改正，给予警告； ■ 拒不改正或者导致危害网络安全等后果的，处 10-100 万元罚款； ■ 对直接负责的主管人员处 1-10 万元罚款。
从事网络产品安全漏洞发现、收集、发布等活动的组织或者个人		■ 设立网络产品安全漏洞收集平台，应当向工业和信息化部备案； ■ 建立健全漏洞信息接收渠道并保持畅通，留存漏洞信息接收日志不少于 6 个月； ■ 加强内部管理，采取措施防范漏洞信息泄露和违规发布； ■ 通过网络平台、媒体、会议、竞赛等方式向社会发布漏洞信息的，应当遵循必要、真实、客观以及有利于防范网络安全风险的原则； ■ 不得在网络产品提供者提供网络产品安全漏洞修补措施之前发布漏洞信息；认为有必要提前发布的，应当与相关网络产品提供者共同评估协商，并向工信部、公安部报告，由工信部、公安部组织评估后进行发布； ■ 不得发布网络运营者在用的网络、信息系统及其设备存在安全漏洞的细节情况；	■ 责令改正，给予警告； ■ 拒不改正或者情节严重的，处 1-10 万元罚款； ■ 可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照； ■ 对直接负责的主管人员和其他直接责任人员处 5,000 元-5 万元罚款。

适用主体	鼓励事项	法律义务	违法后果
		■ 不得刻意夸大网络产品安全漏洞的危害和风险，不得利用网络产品安全漏洞信息实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动； ■ 不得发布或者提供专门用于利用网络产品安全漏洞从事危害网络安全活动的程序和工具； ■ 在发布网络产品安全漏洞时，应当同步发布修补或者防范措施； ■ 在国家举办重大活动期间，未经公安部同意，不得擅自发布网络产品安全漏洞信息； ■ 不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。	
其他组织或个人	■ 向网络产品提供者通报其产品存在的安全漏洞； ■ 向工信部网络安全威胁和漏洞信息共享平台、国家网络与信息安全信息通报中心漏洞平台、国家计算机网络应急技术处理协调中心漏洞平台、中国信息安全测评中心漏洞库报送网络产品安全漏洞信息。	■ 不得利用网络产品安全漏洞从事危害网络安全的活动； ■ 不得非法收集、出售、发布网络产品安全漏洞信息； ■ 明知他人利用网络产品安全漏洞从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。	**尚不构成犯罪的：** ■ 没收违法所得，处 5 日以下拘留；可以并处 5-50 万元罚款； ■ 情节较重的，处 5-15 日拘留；可以并处 10-100 万元罚款。 **单位有前款行为的：** ■ 没收违法所得； ■ 处 10-100 万元罚款； ■ 并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 **相关人员：** ■ 受到治安管理处罚的人员，5 年内不得从事网络安全管理和网络运营关键岗位的工作； ■ 受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

特别声明

汉坤律师事务所编写《汉坤专递》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤律师事务所的下列人员联系：

北京　金文玉　律师：

电话：　+86 10 8525 5557

Email：　wenyu.jin@hankunlaw.com

上海　曹银石　律师：

电话：　+86 21 6080 0980

Email：　yinshi.cao@hankunlaw.com

深圳　王哲　律师：

电话：　+86 755 3680 6518

Email：　jason.wang@hankunlaw.com

香港　陈达飞　律师：

电话：　+852 2820 5616

Email：　dafei.chen@hankunlaw.com