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

关键信息基础设施安防重器——详解《网络安全审查办法》

作者：潘永建 | 孔焕志 | 王雪莹 | 沙莎 | 胡鑫超

网络产品和服务的安全性是确保网络安全的前提。我国网络安全法律体系中，网络设备、产品和服务的安全审查主要包括两部分内容：对网络关键设备和网络安全专用产品的检测和认证[1]，以及对关键信息基础设施运营者(以下简称“CIIO”)采购网络产品和服务的安全审查。新颁布的《网络安全审查办法》[2](以下简称“《办法》”)即是关于后者的重要制度。

《办法》由国家互联网信息办公室(以下简称“国家网信办”)、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局(以下简称“十二部委”)联合制定，将于 2020 年 6 月 1 日正式实施，《网络产品和服务安全审查办法(试行)》(2017 年)(以下简称“《试行办法》”)将被同时废止。

为撰此文，笔者比较《办法》与之前颁布的《试行办法》和《网络安全审查办法(征求意见稿)》(2019 年)(以下简称“《征求意见稿》”)的异同，对照网络安全法律体系相关法规，并结合笔者从业的实务经验，旨在帮助企业正确、全面理解网络安全审查制度。

[1] 关于网络关键设备和网络安全专用产品的检测和认证问题，请参见通力合规团队《网络设备、产品与服务的安全审查制度》一文。
[2] 《网络安全审查办法》全文: http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

一. 主要内容

1. 立法目的和制定依据

《办法》第 1 条明确立法目的是“确保关键信息基础设施供应链安全，维护国家安全”。在各经济体互融互进的大背景下，国家坚持对外开放方针的同时，如何维护网络安全是技术和制度上的难题，保护关键信息基础设施更是其中至关重要的一环。早在 2016 年颁布的《国家网络空间战略》便要求“建立实施网络安全审查制度，加强供应链安全管理，对党政机关、重点行业采购使用的重要信息技术产品和服务开展安全审查，提高产品和服务的安全性和可控性”。

关于制定依据，《试行办法》和《征求意见稿》都采用“依据《国家安全法》《网络安全法》等法律法规”的表述，而《办法》删去“等法律法规”字词，而明确《国家安全法》第 59 条和《网络安全法》第 35 条是网络安全审查的直接依据。相应地，《办法》在第 2 条中删除“法律、行政法规另有规定的，依照其规定”的表述。国家网信办有关负责人在《<网络安全审查办法>答记者问》(以下简称“《答记者问》”)中亦明确了上述调整。无疑，这些调整增加了《办法》在适用和解释方面的确定性。

2. 审查对象

相较于《试行办法》，《办法》对界定网络安全审查对象范围的标准有所变化。《试行办法》规定“关系国家安全的网络和信息系统采购的重要网络产品和服务”均应经过网络安全审查。换言

之，不限于 CIIO，其他运营者只要符合“关系国家安全的网络和信息系统”的标准，也可能是网络安全审查的义务主体。

《办法》对受审查的采购主体进行了限缩规定，并对采购内容进行了列举说明。只有采购主体和采购内容落入以下范围，且采购活动“影响或可能影响国家安全的”，才具有网络安全审查的申报义务。

(1) 采购主体: CIIO。关于 CIIO 的认定方法和步骤，详见本文后部分内容。
(2) 采购内容: 主要指核心网络设备、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。

3. 审查主体

(1) 申报受理部门: 网络安全审查办公室。网络安全审查办公室设在国家网信办。
(2) 具体工作承担部门: 中国网络安全审查技术与认证中心。中国网络安全审查技术与认证中心在网络安全审查办公室的指导下，承担接收申报材料、对申报材料进行形式审查、具体组织审查工作等任务。
(3) 其他参与机关: 中央网络安全和信息化委员会、网络安全审查工作机制成员单位(由十二部委在中央网络安全和信息化委员会领导下建立)和相关关键信息基础设施保护工作部门。

4. 审查程序

网络安全审查的程序规定在《办法》第 5 条至第 15 条中。网络安全审查可以依申报或依职权启动，具体的审查程序请参考附录流程图。CIIO 应当对《办法》和《答记者问》中指出的申报时间和申报材料的建议和要求予以关注和重视:

(1) 申报时间: 通常情况下，CIIO 应当在与产品和服务提供方(以下简称“提供方”)正式签署合同前申报网络安全审查。
(2) 申报材料: 申报书; 关于影响或可能影响国家安全的分析报告; 采购文件、协议、拟签订的合同等; 网络安全审查工作需要的其他材料。关于“网络安全审查工作需要的其他材料”，我们认为需要参考 CIIO 所在行业的特殊监管要求，以及如果采购的网络产品和服务属于网络关键设备、网络安全专用产品，可能需要提供其符合法律、行政法规的规定和相关国家标准的强制性要求的证明。[3]

5. 审查标准

《办法》第 9 条以“列举+兜底”的方式规定了网络安全审查办公室在评估采购网络产品和服务可能带来的国家安全风险时主要考虑的因素:

[3] 《信息安全技术 关键信息基础设施网络安全保护要求》(征求意见稿)第 4.3.15 条: 运营者采购、使用的网络产品和服务，尤其是网络关键设备、网络安全专用产品，应符合法律、行政法规的规定和相关国家标准的强制性要求。

(1) 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;
(2) 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;
(3) 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;
(4) 产品和服务提供者遵守中国法律、行政法规、部门规章情况;
(5) 其他可能危害关键信息基础设施安全和国家安全的因素。

相较于《征求意见稿》，《办法》删除了“导致个人信息泄露、丢失、毁损、出境等的可能性”“对国防军工、关键信息基础设施相关技术和产业的影响”“产品和服务提供者承诺承担的责任和义务”“产品和服务提供者受外国政府资助、控制等情况”等条款。立法者对这些条款的删除可能出于多种原因。需要说明的是，尽管有上述删除，但企业不可忽视其他法律规范已作出的特殊规定。例如，人类遗传资源出境的内容已在《人类遗传资源管理条例》中予以调整规制。

6. 监管方式

《办法》第 3 条提出网络安全审查以“事前审查与持续监管相结合、企业承诺与社会监督相结合”为原则，在此基础上赋予了网络安全审查办公室事前事中事后监督的职责。表面上看，网络安全审查集中在采购阶段，但实质上，监督贯穿网络产品和服务的整个生命周期：事前通过审查采购合同，预估风险；事中事后要求 CIIO 督促提供方履行网络安全审查中作出的承诺，以合同为纽带约束提供方的行为，使得网络安全审查由“节点控制”延伸为“过程控制”。

在监管方式方面，《办法》中规定网络安全审查办公室以“接受举报”的方式进行监督，删去了《征求意见稿》中规定的“抽查”形式。

7. 违法责任

CIIO 应当申报网络安全审查而没有申报的，或者使用网络安全审查未通过的产品和服务的法律责任规定在《办法》第 19 条(责令停止使用相关产品和服务，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款)。可以看出，CIIO 和直接责任人员均应对不合规的采购行为负责。

二. 重点解读

1. CIIO

《答记者问》中提及 CIIO 的范围，即 CIIO 指“电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统运营者”，但由于其采用“等行业领域”“重要网络和信息系统运营者”的不确定表述，我们理解前述具体行业的运营者尚无法涵盖所有的义务主体，且这些行业内的网络运营者并非一概属于义务主体。

目前法律法规对 CIIO 尚无明确的定义，实践中通常从关键信息基础设施的定义出发以确定其运营者的范围，但法律对关键信息基础设施的定义范围仅作出了较为原则性的定义，缺乏明确的认定标准。《网络安全法》规定，“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，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、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”类似地，《国家网络空间安全战略》和《关键信息基础设施安全保护条例(征求意见稿)》也各自通过“行业列举+后果概括”的复合定义方式，在《网络安全法》提出的行业基础上进一步扩增了部分其他领域的工业系统和信息系统。

此外，政府部门的若干工作指南中确立了初步识别关键信息基础设施的步骤：首先确定关键业务，其次确定支撑关键业务的信息系统或工业控制系统，最后判断一旦发生网络安全事故可能造成的影响。因此，并非所有落入法规列举的行业的网络运营者，就必然属于 CIIO。未落入法规列举的行业的网络运营者，也有可能因其网络设施和信息系统遭到破坏、丧失功能或者数据泄露，对国家安全、国计民生、公共利益造成严重危害，从而构成 CIIO。识别关键信息基础设施的详细步骤请参见通力合规团队《关键信息基础设施的界定》一文。

值得注意的是，《办法》虽仍未提出 CIIO 的认定标准，但明确指出 CIIO 由关键信息基础设施保护工作部门认定，这在一定程度上为网络运营者判断其是否属于 CIIO 提供了参照和指引。

2. 影响或可能影响国家安全

在信息时代，网络安全于国家安全而言，牵一发而动全身，同国家安全的许多方面都有着密切关系，网络安全事件可能产生广泛的社会影响。例如 2019 年 3 月，委内瑞拉被黑客攻击发生电力系统崩溃事件，该国大多数区域受停电影响，引发交通瘫痪、地铁系统关闭、医院手术中断、所有通讯线路中断、航班无法正常起降等社会秩序混乱。网络安全可能造成的国家安全影响，在《办法》第 9 条的网络安全审查内容中有所体现，主要为关键信息基础设施被非法控制、遭受干扰或破坏，重要数据被窃取、泄露、毁损，关键信息基础设施业务或供应中断，和提供方违反中国法律、行政法规、部门规章等造成的国家安全危害。

另一方面，《办法》第 5 条规定 CIIO 有义务预判采购的网络产品和服务投入使用后可能带来的国家安全风险。我们理解，各行业由于各自复杂的经营环境和实际情况，面临不同的国家安全风险，因此，此次颁布的《办法》删去了《征求意见稿》中预判相关安全风险的参照情形，而提出由关键信息基础设施保护工作部门制定本行业、本领域的预判指南。但在关键信息基础设施保护工作部门出台这些预判指南前，《征求意见稿》提出的网络安全审查考量因素具有一定的参考价值，包括关键信息基础设施整体停止运转或主要功能不能正常运行，大量个人信息和重要数据泄露、丢失、毁损或出境，或者关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁等。

3. 关键信息基础设施保护工作部门

根据《办法》，关键信息基础设施保护工作部门将在国家安全审查工作中发挥重要作用，作为CIIO 的认定部门，其不仅有权制定本行业、本领域预判指南，为 CIIO 进行网络安全审查申报提供依据，还将直接参与到网络安全审查中，对网络安全审查办公室作出的审查结论建议提出书面回复意见。事实上，“关键信息基础设施保护工作部门”的表述自《试行办法》《征求意见稿》沿用至《办法》，但均未明确具体哪些部门属于关键信息基础设施保护工作部门。

根据《关键信息基础设施安全保护条例(征求意见稿)》第 19 条的规定，“国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施”。我们理解，网络安全法律体系内各法规对相关概念的规定应是一致的。因此，关键信息基础设施保护工作部门指的应是国家行业主管或监管部门。实践中，也的确是国家行业主管或监管部门在承担关键信息基础设施保护工作部门的职责。例如，水利部在 2020 年 2 月 14 日发布的《2020 年水利网信工作要点》中指出，“落实关键信息基础设施保护工作部门职责，制定《水利关键信息基础设施网络安全建设指导意见》，完成摸底风险评估。依据《水利关键信息基础设施认定规则》，全面梳理排查大型水利枢纽及引调水工程，进一步筛选水利关键信息基础设施。”由于《关键信息基础设施安全保护条例》仍处于征求意见稿阶段，关键信息基础设施保护工作部门的含义仍需通过法律法规和相关部门实践予以最终明确。

4. 重要数据

国家安全审查考虑的主要因素之一是“重要数据被窃取、泄露、毁损的风险”。《网络安全法》第 37 条即提出了 CIIO 应当在境内存储在境内运营中收集和产生的重要数据的要求，但何为重要数据，《网络安全法》未直接给出定义。

国家网信办在 2017 年发布的《个人信息和重要数据出境安全评估办法(征求意见稿)》中对重要数据作出定义，指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。此处提到的“重要数据识别指南”是指推荐性国标《信息安全技术 数据出境安全评估指南(征求意见稿)》的附录。该附录中列明 26 个不同行业(领域)重要数据判定的主管部门，并列举了重要数据的类型，具有重要参考价值。此外，2019 年发布的《数据安全管理办法(征求意见稿)》第 38 条指出，“重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。”

我们理解，重要数据具有行业特殊性，行业主管部门有权结合相关行业规定，进一步明确行业内的重要数据具体定义、范围及判定依据。重要数据的判定应着眼于国家安全、国计民生及公共利益整体层面的利益保护。若不涉及该等整体层面利益的数据，则不应落入重要数据的范畴。可能构成 CIIO 的企业，可以根据其所处的行业，业务所涉猎的行业，业务规模，所收集的数据类型、体量、性质，综合判断其运营过程中收集、产生的数据是否属于重要数据。在需要的情况下，可以通过与行业主管部门积极沟通，有效识别重要数据。识别重要数据的详细内容请参见通力合规团队《重要数据概念辨析与识别》一文。

5. 无关方

根据《办法》第 16 条和第 17 条的规定，参与审查的机构和人员应当严格保护企业商业秘密和知识产权，未经信息提供方同意，不得向无关方披露，如果审查人员未能正确履行保密义务，则 CIIO 或提供方均可向网络安全审查办公室和相关部门进行举报。上述两条规定不仅对审查人员提出了保密的要求，也为信息提供方提供了救济途径，无疑为 CIIO 和提供方的商业秘密和知识产权撑起保护伞。尽管如此，实践中该保护伞的救济可能存在以下两个悬而未决的问题。

第一，无关方的定义和范围。从《办法》的规定来看，可能接触到信息提供方的商业秘密和知识产权的机构包括网络安全审查办公室、网络安全审查工作机制成员单位、行业主管部门和中央网络安全和信息化委员会。那么，无关方是否可以等同于上述四类主体以外的任何部门和人员；如果商业秘密和知识产权被其他任何部门和人员知悉，是否可以认定审查部门和审查人员违反保密义务，这些答案并不明确。因此，实践中需要继续澄清保密义务延伸的程度，以及明确无关方认定的具体标准。

第二，违反保密义务的后果。从第 17 条的规定来看，CIIO 和提供方可以对审查人员违反保密义务的行为进行举报，但遗憾的是，《办法》并未进一步说明其违反的法律责任。结合《刑法》《外商投资法》《行政机关公务员处分条例》的规定，我们认为，行政机关工作人员可能面临处分，构成犯罪的需要承担刑事责任，但 CIIO 和提供方是否有权因审查人员违反保密义务而提起国家赔偿尚未可知。根据《国家赔偿法》的规定，受害人可以依据行政机关以下侵犯财产权的行为获得赔偿：违法实施行政处罚、违法采取行政强制措施、违法征收征用财产和其他造成财产损害的行为。审查人员仅在审查过程中泄露 CIIO 的商业秘密，是否可以纳入其他造成财产损害的行为，以及 CIIO 和提供方是否具有其他获取赔偿的方式，有待在实践中查明。

三. 企业合规建议

1. CIIO

(1) 在采购网络产品和服务前对提供方开展背景调查，确保提供方具有履行相关承诺的资信及能力，了解外国政府对提供方经营的资助、控制和影响情况。就网络产品和服务，尤其是网络关键设备、网络安全专用产品，应符合法律、行政法规的规定和相关国家标准的强制性要求，并应在其上线应用前进行安全检测。

(2) 对采购网络产品和服务的国家安全风险进行预判，国家安全审查的因素将是预判国家安全风险的重要参照，CIIO 应密切关注相关部门未来出台的预判指南。

(3) 在与产品和服务提供方正式签署合同前申报网络安全审查。如果在签署合同后申报网络安全审查，建议在合同中注明此合同须在产品和服务采购通过网络安全审查后方可生效，以避免因未通过网络安全审查而承担违约责任。

根据《办法》的规定，CIIO 签订合同后，如果需要进行一般审查，则从提交申请到审查结束可能等待的最长时间为 70(10+45+15)日；而特别程序审查程序中，需等待的时间为115(70+45)日甚至更长(以上不包括提交补充材料的时间)。这表明企业在签订采购合同后可能面临长达三个月的安全审查时间。因此，CIIO 应当在签订合同前妥善设置合同条款，将通过安全审查作为合同生效的要件。此外，提交安全审查前，应当尽量备齐待审查材料，节省后期可能因补充材料而耗费的时间。

(4) 在采购合同等文件中明确提供方的安全责任和义务，与提供方签订安全保密协议。安全保密协议可参考《信息安全技术 关键信息基础设施网络安全保护基本要求(征求意见稿)》的模板。

(5) 在实际使用网络产品和服务过程中，CIIO 应督促提供方履行网络安全审查中作出的承诺，预防提供方非法获取用户数据、非法控制和操纵用户设备、无正当理由中断产品供应和必要的技术支持服务的情况。当发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向安全保护工作部门报告。

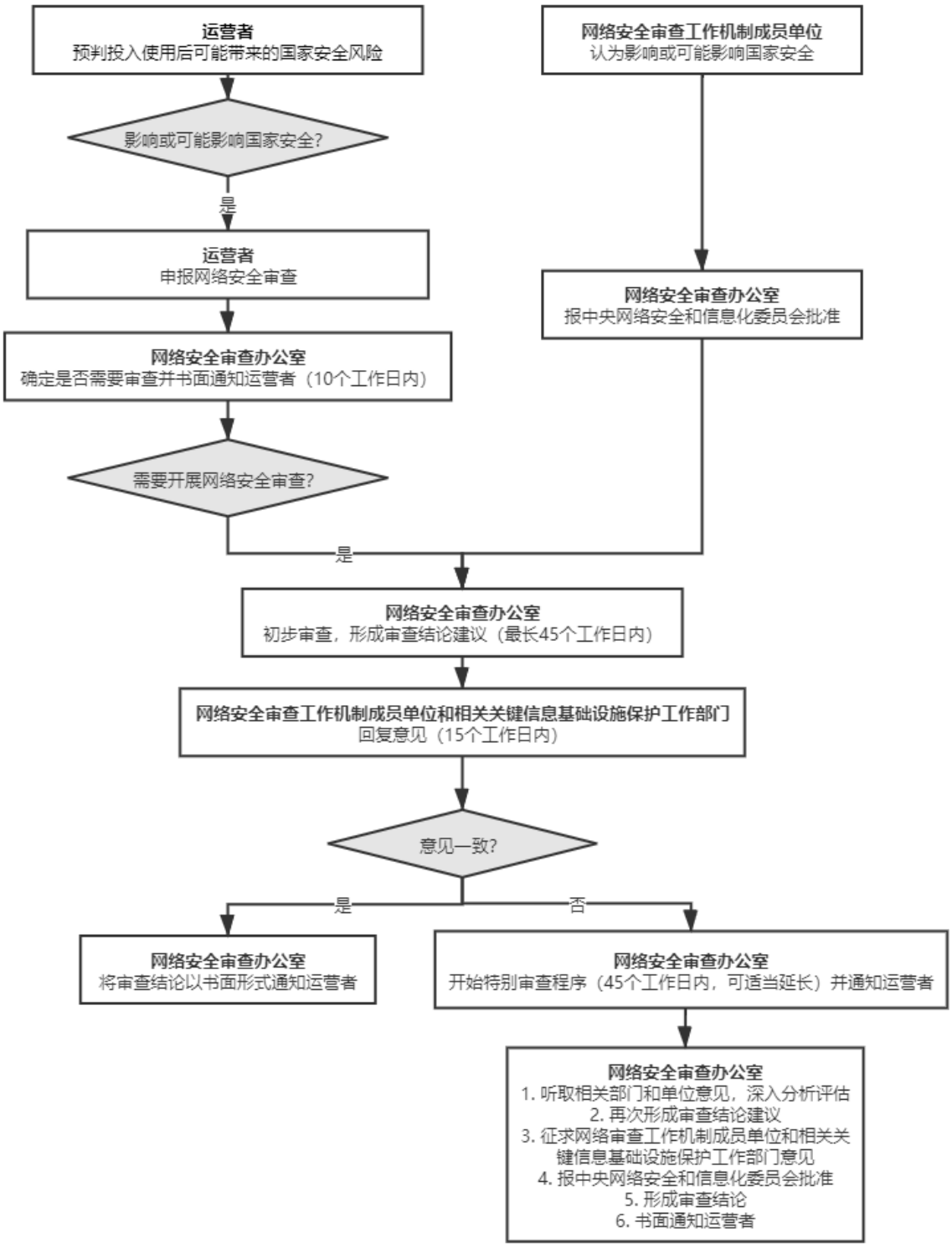
2. 提供方

(1) 提供方应当签署合规的承诺文件，配合网络安全审查，严格履行网络安全审查中作出的承诺，遵守涉及用户数据、用户设备、产品供应与技术支持等合同内容。

(2) 提供方自身经营过程中应遵守中国法律、行政法规、部门规章，提供的相关产品及服务应当符合中国的准入要求，具备相应资质，遵从网络安全等级保护、个人信息保护、数据本地化存储等网络安全领域的合规要求，避免因行政、刑事处罚等“违法前科”影响交易。

(3) 提供方还可参照《信息安全技术 网络产品和服务安全通用要求(征求意见稿中)》中的安全保障要求，在恶意程序防范、缺陷漏洞管理、用户信息保护等方面进行完善，切实做到合法合规。

附录:


运营者
预判投入使用后可能带来的国家安全风险
影响或可能影响国家安全?
是
运营者
申报网络安全审查
网络安全审查办公室
确定是否需要审查并书面通知运营者（10个工作日内）
需要开展网络安全审查?
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
网络安全审查办公室
报中央网络安全和信息化委员会批准
是
网络安全审查办公室
初步审查，形成审查结论建议（最长45个工作日内）
网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门
回复意见（15个工作日内）
意见一致?
是
否
网络安全审查办公室
将审查结论以书面形式通知运营者
网络安全审查办公室
开始特别审查程序（45个工作日内，可适当延长）并通知运营者
网络安全审查办公室
1. 听取相关部门和单位意见，深入分析评估
2. 再次形成审查结论建议
3. 征求网络审查工作机制成员单位和相关关键信息基础设施保护工作部门意见
4. 报中央网络安全和信息化委员会批准
5. 形成审查结论
6. 书面通知运营者

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

孔焕志
+86 21 3135 8777
kenneth.kong@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