2022 版《网络安全审查办法》重点问题评析

作者：潘永建 | 杨迅 | 朱晓阳 | 左嘉玮

2021 年 7 月 10 日，国家互联网信息办公室(“国家网信办”)发布《网络安全审查办法(修订草案征求意见稿)》(“《修订草案》”)，对实施刚满一年的《网络安全审查办法(2020)》(“《2020 办法》”)进行了实质性的修订。经过近半年时间的酝酿，2022 年 1 月 4 日，国家网信办等十三部门正式发布修订后的《网络安全审查办法》(“《办法》”)。在本文中，通力合规团队将解读《办法》的立法沿革、重点修改以及网络安全审查的具体程序和后果，以期为企业提供合规指引。

目录

一. 立法沿革
二. 重点修改
- 将数据处理活动纳入审查范围
- 赴国外上市须申报审查
- 特别审查程序时限延长
- 依职权审查时，当事人有义务预防和消减风险

三. 网络安全审查的具体程序及后果
四. 附录：《网络安全审查办法》修订对比

一. 立法沿革

网络安全审查制度源于 2016 年颁布的《网络安全法》(“《网安法》”)。为加强关键信息基础设施安全保护，《网安法》第二十五条规定，关键信息基础设施的运营者(“CIIO”)采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。为落实这一规定，国家网信办制定《网络产品和服务安全审查办法(试行)》，于 2017 年 6 月 1 日与《网安法》同日实施。2020 年，在总结实践经验的基础上，国家网信办等 12 部门联合制定了《2020 办法》，对网络安全审查对象、程序、标准等进行了细致的规定。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

2021 年 6 月 10 日,《数据安全法》(“《数安法》”)正式颁布,明确规定国家建立数据安全审查制度。《数安法》颁布一月之际,国家首次实施网络安全审查制度。2021 年 7 月 2 日,网络安全审查办公室发布公告,宣布对“滴滴出行”实施网络安全审查,这是《网安法》确立网络安全审查制度以来,首次对外公布的审查行动。2021 年 7 月 10 日,为进一步落实《数安法》要求,国家网信办发布了《网络安全审查办法(修订草案征求意见稿)》,将数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围,并针对企业赴国外上市等场景作出了特别规定。近日,修订后的《办法》正式颁布,并将于 2022 年 2 月 15 日起施行。

二. 重点修改

与《2020 办法》相比,新颁布的《办法》在以下方面进行了重点修改:

- **将数据处理活动纳入审查范围**
- **赴国外上市须申报审查**
- **特别审查程序时限延长**
- **依职权审查时,当事人有义务预防和消减风险**

将数据处理活动纳入审查范围

为了进一步保障网络安全和数据安全,《办法》将“网络平台运营者开展数据处理活动影响或者可能影响国家安全”等情形纳入网络安全审查范围。相应的,《办法》第二条新增“网络平台运营者”作为审查的适用对象,与 CIIO 一并统称为“当事人”。然而,《办法》并没有对“网络平台运营者”进行详细定义。虽然此前《互联网平台落实主体责任指南(征求意见稿)》《网络数据安全管理条例(征求意见稿)》等规定对“互联网平台运营者”进行了较为明确的界定[1],但“互联网平台”与“网络平台”并不完全相同,相关概念仍有待监管部门进一步厘清。现阶段,我们建议企业不应过度关注自身是否属于“网络平台运营者”,而应该根据数据处理活动所涉及的风险程度来判断是否需要申报审查。

在审查内容上,《办法》也特别强调了对于数据安全的关注,将《2020 办法》中的“重要数据被窃取、泄露、毁损的风险”扩充为“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”。

此外,《办法》第二十二条第二款指出,国家对数据安全审查、外商投资安全审查另有规定的,应当同时符合其规定。换言之,网络安全审查的适用范围并不限于《办法》中已列明的情形。今后,监管部门可能会在数据安全、外商投资相关审查办法中,提出网络安全审查的要求。

[1]《互联网平台落实主体责任指南(征求意见稿)》附则:(2) 平台经营者,是指向自然人、法人及其他市场主体提供经营场所、交易撮合、信息发布等互联网平台服务的法人及非法人组织。通过互联网等信息网络从事销售商品或者提供服务的自建网站经营者,可参照平台经营者适用本指南。
《网络数据安全管理条例(征求意见稿)》第七十三条:(九) 互联网平台运营者是指为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者。

例如, 2021 年实施的《外商投资安全审查办法》明确将“(外国投资者)投资关系国家安全的重要农产品、重要能源和资源、重大装备制造、重要基础设施、重要运输服务、重要文化产品与服务、重要信息技术和互联网产品与服务、重要金融服务、关键技术以及其他重要领域，并取得所投资企业的实际控制权”列为应当主动申报外商投资安全审查的情形。[2]结合《办法》的立法精神，预计将来在“外国投资者通过并购方式取得境内企业的实际控制权”的场景中，若被投资企业构成 CIIO 或网络平台运营者，则很可能需要同时进行网络安全审查。

赴国外上市须申报审查

《办法》指出，掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查，并相应地将中国证券监督管理委员会纳入“网络安全审查机制成员单位”。根据《办法》第十条，审查的一个关键因素是“上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险。”

鉴于《网络数据安全管理条例(征求意见稿)》在第十三条中明确区分了“赴国外上市”和“赴香港上市”两种场景下的网络安全审查申报标准。[3]《办法》相关条款表明，企业在赴香港上市时，如果不影响国家安全，申报网络安全审查并非强制性要求。但值得注意的是，在赴香港上市的过程中，如涉及跨境传输等数据处理活动，仍需遵守法律法规关于数据出境的规定。

在《<网络安全审查办法>答记者问》一文中，国家网信办有关负责人具体说明了赴国外上市时的申报时机以及可能的结果。[4]网络平台运营者应在向国外证券监管机构提出上市申请之前，申报网络安全审查，并提交包括“拟提交的首次公开募股(IPO)等上市申请文件”在内的相关材料。申报网络安全审查可能有以下三种情况：一是无需审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。

特别审查程序时限延长

《办法》第十四条对特别审查程序的完成时限进行了调整，将《2020 办法》规定的 45 个工作日延长为 90 个工作日。

[2] 参见《外商投资安全审查办法》第四条
[3] 《网络数据安全管理条例(征求意见稿)》第十三条 数据处理者开展以下活动，应当按照国家有关规定，申报网络安全审查:
(一)汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立，影响或者可能影响国家安全的;
(二)处理一百万人以上个人信息的数据处理者赴国外上市的;
(三)数据处理者赴香港上市，影响或者可能影响国家安全的;
(四)其他影响或者可能影响国家安全的数据处理活动。
大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。
[4] http://www.cac.gov.cn/2022-01/04/c_1642894602460572.htm

在我国网络安全审查制度中，分为一般审查程序以及在“相关网络安全审查部门意见不一致时”启动的特别审查程序[5]。考虑到修订后的《办法》涉及的审查情形增加，特别是可能涉及到企业赴国外上市等复杂情形，国家网信办适当的延长了特别审查程序的时限。

依职权审查时，当事人有义务预防和消减风险

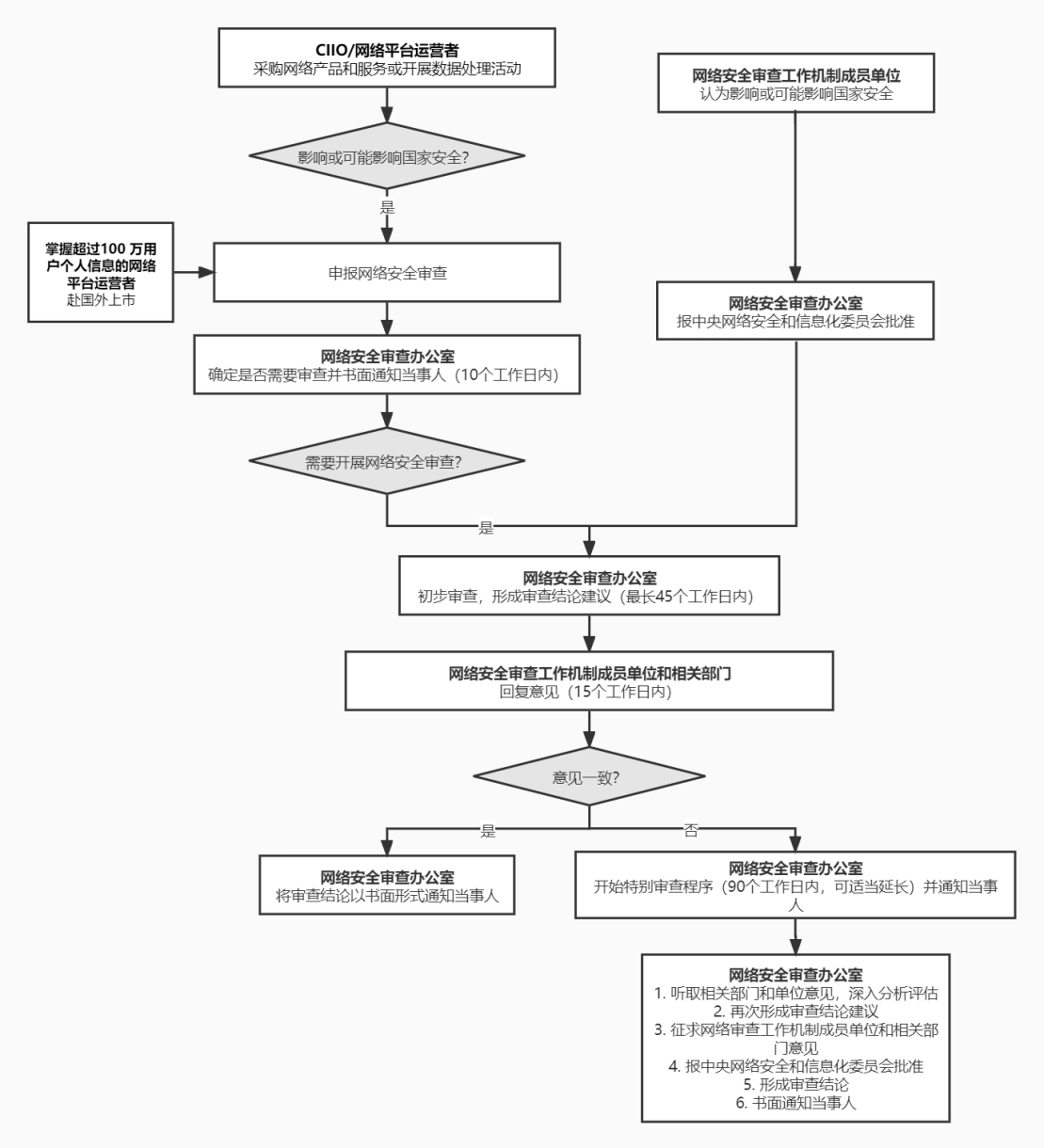
根据《办法》第十六条(《2020 办法》第十五条)，除了依当事人申请进行审查外，网络安全审查办公室也可以依职权进行审查。此外，《办法》在第十六条新增一款，规定“为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施”。

根据国家网信办在对“滴滴出行”等企业进行网络安全审查的过程中发布的一系列通报，上述措施可能包括但不限于从应用商店下架 App、停止新用户注册等。这意味着，在网络安全审查办公室依职权启动的审查中，被审查的企业可能会面临严重的业务连续性问题。

三. 网络安全审查的具体程序及后果

修订后，网络安全审查具体的审查程序如下图所示:

[5] 参见《办法》第十二条



网络安全审查启动后，对于情况复杂的，企业可能面临 150 天(45+15+90)甚至更长时间的审查。在此期间，对于依申请进行的网络安全审查，企业可能无法在审查期间内签署网络产品与服务的供应合同、开展相应的数据处理活动或完成上市程序；对于依职权进行的网络安全审查，企业的日常业务也可能受到相应影响。

《办法》第二十条指出，当事人违反办法规定的，依照《网安法》《数安法》的规定处理。根据《网安法》第六十五条，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，由有关主管部门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)。

对于网络平台运营者违反《办法》规定时的责任，目前《数安法》等法律尚未有对应的规定。《网络数据安全管理条例(征求意见稿)》第六十条规定了相应的罚则，企业未按照国家有关规定申报网络安

全审查的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者导致危害数据安全等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、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五万元以上二十万元以下罚款。

为了给网络安全审查制度提供执法依据，国家网信办可能会尽快出台《网络数据安全管理条例》。届时，无论是 CIIO 或网络平台运营者，若未按要求申报网络安全审查，相关的企业和直接责任人员均应对违规行为负责。

四. 附录：《网络安全审查办法》修订对比：

网络安全审查办法(2020) 2020.06.01 施行	网络安全审查办法(2022) 2022.02.15 施行
第一条 为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》，制定本办法。	**第一条** 为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，根据《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》，制定本办法。
第二条 关键信息基础设施运营者(~~以下简称运营者~~)采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。	**第二条** 关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。 前款规定的关键信息基础设施运营者、网络平台运营者统称为当事人。
第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。	**第三条** 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。
第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民	**第四条** 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和

共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、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、国家密码管理局建立国家网络安全审查工作机制。 **网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。**	国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局建立国家网络安全审查工作机制。 网络安全审查办公室设在国家互联网信息办公室，负责制定网络安全审查相关制度规范，组织网络安全审查。
第五条 运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。 关键信息基础设施保护工作部门可以制定本行业、本领域预判指南。	**第五条** 关键信息基础设施运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。 关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。
第六条 对于申报网络安全审查的采购活动，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查，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。	**第六条** 对于申报网络安全审查的采购活动，关键信息基础设施运营者应当通过采购文件、协议等要求产品和服务提供者配合网络安全审查，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者必要的技术支持服务等。
	第七条 掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。
~~**第七条** 运营者~~申报网络安全审查，应当提交以下材料: (一)申报书; (二)关于影响或可能影响国家安全的分析报告; (三)采购文件、协议、拟签订的合同等; (四)网络安全审查工作需要的其他材料。	**第八条** 当事人申报网络安全审查，应当提交以下材料: (一)申报书; (二)关于影响或者可能影响国家安全的分析报告; (三)采购文件、协议、拟签订的合同或者拟提交的首次公开募股(IPO)等上市申请文件; (四)网络安全审查工作需要的其他材料。

~~第八条~~ 网络安全审查办公室应当自收到审查申报材料起，10 个工作日内确定是否需要审查并书面通知~~运营者~~。	第九条 网络安全审查办公室应当自收到符合本办法第八条规定的审查申报材料起 10 个工作日内，确定是否需要审查并书面通知当事人。
~~第九条~~ 网络安全审查重点评估采购~~网络产品和服务~~可能带来的国家安全风险，~~主要考虑~~以下因素： (一)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； (二)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； (三)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； (四)产品和服务提供者遵守中国法律、行政法规、部门规章情况； (五)其他可能危害关键信息基础设施安全和国家安全的因素。	第十条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素： (一)产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险； (二)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； (三)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； (四)产品和服务提供者遵守中国法律、行政法规、部门规章情况； (五)核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险； (六)上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险； (七)其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。
~~第十条~~ 网络安全审查办公室认为需要开展网络安全审查的，应当自向~~运营者~~发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送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~~部门征求意见；情况复杂的，可以延长 15 个工作日。	第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长 15 个工作日。
~~第十一条~~ 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~~部门应当自收到审查结论建议之日起 15 个工作日内书面回复意见。 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~~部门意见一致的，网络安全审	第十二条 网络安全审查工作机制成员单位和相关部门应当自收到审查结论建议之日起 15 个工作日内书面回复意见。 网络安全审查工作机制成员单位、相关部门意见一致的，网络安全审查办公室以书面形式将审

查办公室以书面形式将审查结论通知~~运营者~~；意见不一致的，按照特别审查程序处理，并通知~~运营者~~。	查结论通知当事人；意见不一致的，按照特别审查程序处理，并通知当事人。
~~第十二条~~ 按照特别审查程序处理的，网络安全审查办公室应当听取相关部门和单位意见，进行深入分析评估，再次形成审查结论建议，并征求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~~部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知~~运营者~~。	**第十三条** 按照特别审查程序处理的，网络安全审查办公室应当听取相关单位和部门意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知当事人。
~~第十三条~~ 特别审查程序一般应当在~~45~~个工作日内完成，情况复杂的可以~~适当~~延长。	**第十四条** 特别审查程序一般应当在 90 个工作日内完成，情况复杂的可以延长。
~~第十四条~~ 网络安全审查办公室要求提供补充材料的，~~运营者~~、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。	**第十五条** 网络安全审查办公室要求提供补充材料的，当事人、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。
~~第十五条~~ 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，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。	**第十六条** 网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，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。 为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。
~~第十六条~~ 参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权，对~~运营者~~、产品和服务提供者提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于审查以外的目的。	**第十七条** 参与网络安全审查的相关机构和人员应当严格保护知识产权，对在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或者用于审查以外的目的。
~~第十七条~~ ~~运营者~~或网络产品和服务提供者认为审查人员有失客观公正，或未能对审查工作中获悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。	**第十八条** 当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。
~~第十八条~~ ~~运营者~~应当督促产品和服务提供者履行网络安全审查中作出的承诺。	**第十九条** 当事人应当督促产品和服务提供者履行网络安全审查中作出的承诺。

网络安全审查办公室通过接受举报等形式加强事前事中事后监督。	网络安全审查办公室通过接受举报等形式加强事前事中事后监督。
~~第十九条~~ ~~运营者~~违反本办法规定的，依照《中华人民共和国网络安全法》~~第六十五条~~的规定处理。	第二十条 当事人违反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》的规定处理。
~~第二十条~~ ~~本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。~~ 本办法所称网络产品和服务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。	第二十一条 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、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、网络安全和数据安全有重要影响的网络产品和服务。
~~第二十一条~~ 涉及国家秘密信息的，依照国家有关保密规定执行。	第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。 国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。
~~第二十二条~~ ~~本办法自 2020 年 6 月 1 日起实施，《网络产品和服务安全审查办法(试行)》同时废止。~~	第二十三条 本办法自 2022 年 2 月 15 日起施行。2020 年 4 月 13 日公布的《网络安全审查办法》(国家互联网信息办公室、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、国家密码管理局令第 6 号)同时废止。

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

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	深圳
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	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	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	**伦敦**	
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	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 2022