君合研究简讯

2020 年 4 月 28 日

网络安全法律热点问题

采购 CII 相关网络产品及服务应如何实施网络安全审查

——《网络安全审查办法》新规解读

2020 年 4 月 27 日，国家互联网信息办公室等 12 个国家部委联合公布了《网络安全审查办法》（以下简称“**新办法**”），新办法将从 2020 年 6 月 1 日起实施，同时废止自 2017 年 6 月 1 日起实施历时三年的《网络产品和服务安全审查办法（试行）》（以下简称“**试行办法**”）。本文拟梳理新办法设定的网络安全审查制度概要，并经过与试行办法及国家互联网信息办公室于 2019 年 5 月 21 日曾公布的《网络安全审查办法（征求意见稿）》（以下简称“**征求意见稿**”）进行比较，总结新办法的亮点以及今后应关注的问题，以期为企业提供参考。

一、 网络安全审查制度概要

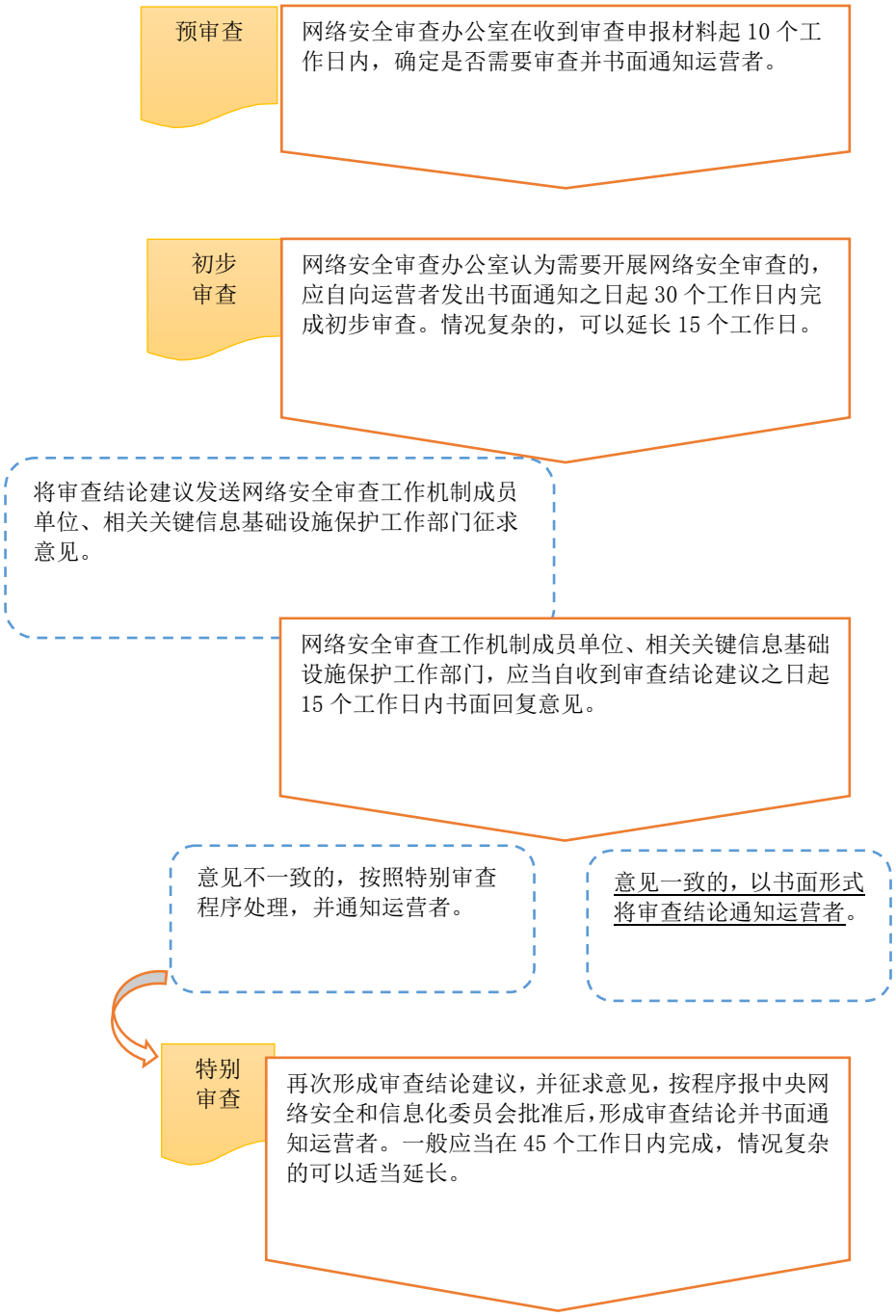
2015 年《国家安全法》实施以来，对影响或可能影响国家安全的网络信息技术产品和服务进行国家安全审查，成为网络安全合规的重要课题。2017 年实施的《网络安全法》第 35 条将实施国家安全审查的场景限定为“关键信息基础设施（简称“**CII**”）的运营者采购网络产品和服务”。但是，《网络安全法》的规定比较原则，没有提及如何实施网络安全审查。根据新办法的相关规定，应按照如下制度框架办理网络安全审查申报手续。

网络安全审查的申报义务人	• **CII 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。** ✓ **CII 运营者是指经 CII 保护工作部门认定的运营者。** ✓ **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 CII 安全有重要影响的网络产品和服务。**

网络安全审查主管部门、工作机制	• 领导部门：由中央网络安全和信息化委员会领导。 • 联合审查工作机制：由国家互联网信息办公室会同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、国家密码管理局等 12 个部局级单位组成国家网络安全审查工作机制。 • 网络安全审查办公室：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。 • 中国网络安全审查技术与认证中心：具体工作委托中国网络安全审查技术与认证中心承担。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[1]。
网络安全审查的申报时点	• 通常情况下，应当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，也可以在签署合同后申报网络安全审查[2]。
网络安全审查的申报材料	• 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。
网络安全审查重点评估的考虑因素	• 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 CII 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 CII 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 CII 安全和国家安全的因素。

[1] 国家互联网信息办公室有关负责人就《网络安全审查办法》答记者问

[2]国家互联网信息办公室有关负责人就《网络安全审查办法》答记者问

网络安全审查流程	
法律责任	CII 的运营者使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，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[3]。

[3]根据《网络安全法》第 65 条

二、 网络安全审查制度的新增关注点

1、 安全审查评估重点考虑“国家安全”

对于“网络产品和服务”的考量方面，新办法在征求意见稿规定的“网络产品和服务的安全性、开放性、透明性”基础上，增加了“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”这些考虑要素[4]。由于近年来的国际贸易保护主义、单边主义倾向增强，包括芯片、高端通信终端等网络产品的国际货物、零部件供应均受到一定程度的影响，受政治、外交等因素导致产品和服务供应链中断的风险在增大，本项规定一定程度上也反映了对这一国际背景的担忧及对策。

此外，新办法明确规定，“产品和服务提供者遵守中国法律、行政法规、部门规章情况”是安全审查评估的考虑因素。因此，运营者向中国境内或境外公司采购网络产品和服务时，需要调查该境外供应商是否遵守中国法律、行政法规、部门规章情况。同时，境外或者外资供应商为了满足上述安全审查合规要求，也应自查对于中国法律、行政法规、规章的遵守情况，如有违反应当及时改正，以免造成不必要的麻烦。

2、 以运营者为直接规制对象、以审查采购合同为手段确保 CII 供应链安全

根据新办法的规定，采购网络产品和服务时，需要履行网络安全审查申报的义务主体是 CII 的运营者，而不是网络产品和服务的提供者。同时，根据新办法规定，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，配合的内容包括：a)产品和服务提供者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，b)产品和服务提供者承诺无正当理由不中断产品供应或必要的技术支持服务等。我们理解，新办法通过要求在采购文件、协议载明 a)和 b)两项内容的方式，为产品和服务提供者设定了义务，实际上是以审查采购合同为手段确保 CII 相关产品、服务供应链的安全。

此外，我们需要注意运营者申报网络安全审查与签订采购合同的先后关系。在征求意见稿中曾要求约定网络安全审查通过后合同方可生效，新办法删除了该条要求，赋予了当事人合同自治的权利，但是国家互联网信息办公室有关负责人就新办法答记者问提到，通常情况下，运营者应当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。对此，关于运营者在提出网络安全审查时应申报的材料，与征求意见稿相比，新办法也相应增加了“拟签订的合同”这一资料。当然，实务中也允许先签署采购合同，然后再申报网络安全审查，但在这种情况下，建议运营者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，以避免因为没有通过网络安全审查而造成损失。

三、 今后应关注的问题

1、 CII 定义有待明确

如前文所述，实施网络安全审查的申报义务主体是 CII 的运营者。但是，相关法律法规对“CII”的界定不够明确。国务院已经将《关键信息基础设施安全保护条例》列入 2019 年立法规划，但目前没有公布最新进展情况，建议企业持续关注最新的立法动向。

《网络安全法》第 31 条以“行业列举+损害程度”的方式，列示了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、公共利益的领域的相关信息基础设施可能构成 CII。在此基础上，国家互联网信息办公室 2017 年 7 月 10 日公布的《关键信息基础设施安全保护条例(征求意见稿)》将应纳入 CII 保护范围的对象扩展到以下领域：

a) 政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

b) 电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；

c) 国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

[4] 《网络安全审查办法》第 9 条（三）

d) 广播电台、电视台、通讯社等新闻单位；

e) 其他重点单位。

此外，部分省区已经实施了 CII 保护试点工作，比如 2018 年云南省召开关键信息基础设施安全保护试点工作部署会，会议公布了入选 CII 试点示范项目的名单，建议企业相应关注地方实务动向。

2、 关注预判指南的制定动向

根据新办法，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。但是，新办法没有规定运营者应从哪些要素着手，来预判产品和服务投入使用后可能产生的国家安全风险。

我们注意到征求意见稿曾规定运营者采购网络产品和服务时，对于可能导致以下情况的，运营者应当向网络安全审查办公室申报网络安全审查，一定程度上提示了预判国家安全风险的相关因素，但是下述 a)-d)项目内容在新办法中没有体现。

a) CII 整体停止运转或主要功能不能正常运行；

b) 大量个人信息和重要数据泄露、丢失、毁损或出境；

c) CII 运行维护、技术支持、升级更新换代面临供应链安全威胁；

d) 其他严重危害 CII 安全的风险隐患。

对此，新办法规定 CII 保护工作部门可以制定本行业、本领域预判指南[5]。因此，建议企业及时关注本行业、本领域的预判指南的立法动向。

3、 对网络安全审查意见的救济措施

对于网络安全审查意见，新办法规定了举报权。新办法第 17 条规定，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。

但是，新办法没有规定举报是否对审查结果产生影响，比如，举报审查人员有失客观公正被证实后，是否可以申请重新审查。也不清楚运营者等是否有权对网络安全审查意见提起包括行政复议以及司法诉讼在内的救济措施。我们注意到《国务院办公厅关于建立外国投资者并购境内企业安全审查制度的通知》中规定，外国投资者并购境内企业行为对国家安全已经造成或可能造成重大影响的，联席会议应要求商务部会同有关部门终止当事人的交易，或采取转让相关股权、资产或其他有效措施，消除该并购行为对国家安全的影响[6]；申请人可向商务部申请修改交易方案或撤销并购交易[7]，但并未赋予申请人提起行政复议或诉讼的救济措施。此外，2020 年 1 月 1 日实施的《外商投资法》明确规定，国家针对外商投资进行安全审查而做出的安全审查决定为最终决定[8]。考虑到网络安全审查涉及国家安全这一特殊事由以及前述立法思路，我们倾向于认为对于网络安全审查的意见也属于最终决定，企业无法通过提起行政复议或者诉讼获得救济。

---

[5] 《网络安全审查办法》第 5 条第 2 款

[6] 《国务院办公厅关于建立外国投资者并购境内企业安全审查制度的通知》第四条（六）

[7] 《国务院办公厅关于建立外国投资者并购境内企业安全审查制度的通知》第四条（四）

[8] 《外商投资法》第 35 条第 2 款

杨锦文　合伙人　电话：86 010 8553 7608　邮箱地址：yangjw@junhe.com
高 健　律　师　电话：86 010 8519 1359　邮箱地址：gaojian@junhe.com