见微知萌—从滴滴出行案谈网络安全审查制度

作者：潘永建 | 朱晓阳 | 邓梓珊 | 沙莎

2021 年 7 月 2 日，网络安全审查办公室发布《网络安全审查办公室关于对“滴滴出行”启动网络安全审查的公告》(以下简称“《公告》”)，宣布对“滴滴出行”实施网络安全审查。7 月 4 日，网信办通知全国各大应用商店下架“滴滴出行”APP。这是《网络安全法》(以下简称“《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，特别是在滴滴刚刚完成其美国 IPO 这一特殊时间点，更是引起了全球对事件本身以及我国网络安全审查制度的高度关注。

关于“滴滴出行”此次为何“突然”被网络安全审查，背后的原因众说纷纭。各路媒体纷纷分析滴滴掌握了何种大数据可能威胁中国国家安全。但无论背后原因如何，滴滴本次被审查无疑与网络及数据安全脱不了干系。本文旨在从“滴滴出行”被审查背后的法律依据、法律原理和可能的法律后果出发，从实务角度解读网络安全审查制度。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

1. 网络安全审查是什么?

我国网络安全法律体系中，存在多种“安全审查”:

(1) 对网络关键设备和网络安全专用产品的检测和认证(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) 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(参见通力合规团队《关键信息基础设施安防重器——详解<网络安全审查办法>》一文);
(3) 对“影响或者可能影响国家安全的数据处理活动”进行的数据安全审查(尚未生效)

此次网络安全审查办公室发布的《关于对“滴滴出行”启动网络安全审查的公告》(以下简称“《公告》”)即是前述第(2)项安全审查，是《网络安全审查办法》(以下简称“《办法》”)所规制的 CIIO 网络安全审查的重要制度。根据《办法》，网络安全审查制度体现为以下特征:

审查对象	• 主体: CIIO • 行为: 采购核心网络设备、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 • 后果: 影响或可能影响国家安全
审查主体	• 受理部门: 网络安全审查办公室 • 执行部门: 中国网络安全审查技术与认证中心 • 其他参与部门: 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
审查启动	• 依申请: CIIO 预判产品和服务投入使用后影响或者可能影响国家安全 • 依职权: 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
审查时限	• 通常情况: 30/45 个工作日(初审)+15 个工作日(书面意见) • 特别审查: 30/45 个工作日(初审)+15 个工作日(书面意见)+45 个工作日(特别审查)+X(情况复杂)
审查结果	• 安全审查通过 • 安全审查未通过: 停止使用，罚款等

2. “滴滴出行”被审查的可能原因?

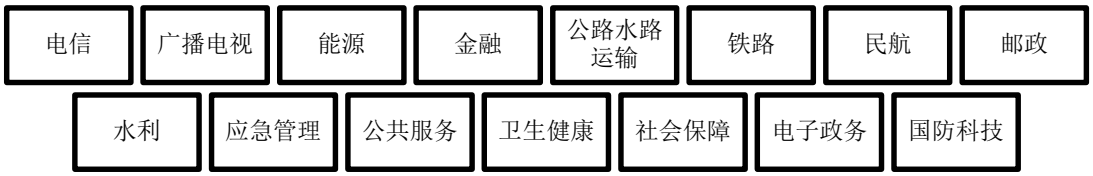
网络安全审查可以依申报或依职权启动。《公告》虽然未明确说明审查的启动方式，但根据《公告》的表述，可以推测出此次针对滴滴的安全审查系依职权的审查。《国家安全法》[1]以及《网安法》[2]作为

[1] 《国家安全法》第五十九条国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险。
[2] 《网络安全法》第三十五条关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家

上位法，为网络安全审查提供了直接依据；《办法》则为网络安全审查的开展提供具体指导。根据前述法律法规的规定，“滴滴出行”被审查的原因可以从以下两个方面进行考虑。

(1) “滴滴出行”很可能构成 CIIO

结合《网安法》以及 2020 年 4 月“国家网络信息办公室有关负责人《网络安全审查办法》答记者问”[3]，以下重点行业领域的重要网络和信息系统[4]运营者构成 CIIO:



尽管目前前述重点行业或领域的主管部门并未公布本部门或本领域的 CIIO 名单或者制定关键信息基础设施的预判指南，但“滴滴出行”作为大型出行和交通平台，其处理的数据包括但不限于用户设备信息、位置信息、行程信息，驾驶员的身份证或其他身份证明、面部识别特征、银行卡信息、信用信息，街景数据、车流数据等，包含了大量的个人信息、个人敏感信息以及重要数据，乃至这些数据融合汇聚而生成的可以反映行业、国家信息的大数据，“滴滴出行”极有可能构成公共服务及交通运输领域的 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)。

(2) “滴滴出行”采购网络产品和服务影响或可能影响国家安全

网络安全审查虽然针对的是 CIIO“采购”网络产品和服务的行为，但审查的重点在于对网络产品和服务的“使用”，而非采购行为本身，只是将安全审查的时点置于 CIIO 的采购行为之前。换言之，网络安全审查办法生效之前 CIIO 已经采购的网络设备或服务，或者 CIIO 应进行审查但未申请审查而擅自采购、使用网络设备或服务的行为，均可落入网络安全审查制度的范围。因此，不排除是滴滴此前已经采购、使用的网络设备和服务触发了本次网络安全审查。

同时，网络安全审查的关注点也绝不是网络设备、服务本身，因为网络设备、服务本身往往并无多大价值，具有价值的是依托于该等设备、服务的数据和背后的关键业务。因此，数据安全也是网络安全审查的一个关注点。

美国证券交易委员会于 2021 年 3 月通过了《外国公司问责法》(Holding Foreign Companies Accountable Act, HFCA)修正案，[5]HFCA 要求外国企业，特别是中国企业必须遵守美国审计标准和

网信部门会同国务院有关部门组织的国家安全审查。

[3] 《网络安全审查办法》答记者问, http://www.cac.gov.cn/2020-04/27/c_1589535446378477.htm

[4] 参照 2020 年 9 月颁布的《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》规定，“符合认定条件的基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等重点保护对象”属于关键信息基础设施。

[5] SEC Issues Amendments, Seeks Public Comment on Holding Foreign Companies Accountable Act,

特定的披露要求。此次“滴滴出行”被安全审查，恰逢其在美上市后不久，引发了“滴滴将数据打包交给美国”的质疑。2021 年 7 月 3 日，“滴滴出行”在其官方微博否认上述猜测，并明确表示“滴滴国内用户的数据都存放在国内服务器，绝无可能把数据交给美国”。

根据《公告》，此次对“滴滴出行”进行网络安全审查的目的是“防范国家数据安全风险，维护国家安全，保护公共利益”。我们认为，分析“滴滴出行”被审的原因，仍应立足于《办法》，不宜对“国家安全”进行泛化理解。需要注意的是，2017 年，“滴滴出行”的关联公司滴图(北京)科技有限公司获得导航电子地图制作的甲级测绘资质，其中包括服务于自动驾驶汽车的高精度地图制作。高精度地图能够精准反映地理位置并记录 GPS 坐标，能够使用激光雷达呈现出目标物精确的三维结构信息，还能获得精准、详尽的道路信息。根据相关法规[6]，我国禁止外商投资“导航电子地图编制”领域；外国组织和个人与中国有关部门和单位合资、合作测绘也不得进行导航电子地图编制活动；未经批准，中国企业用于自动驾驶技术道路测试的地图数据也不得向外国组织和个人提供。“滴滴出行”作为 CIIO，如果在美上市的过程中根据披露要求涉及上述数据，则可能被认定为“影响国家安全”，导致网络安全审查制度的启动。而具体构成“影响国家安全”的情况，我们将在下文进一步展开分析。

3. 网络安全审查，审的是什么?

《办法》开宗明义，网络安全审查以维护国家安全为基石，以确保关键信息基础设施的供应链安全为立足点。根据《审查办法》，评估 CIIO 采购网络产品和服务的国家安全风险时，主要考虑以下因素:

产品和服务使用过程中的风险

- 关键信息基础设施被非法控制、遭受干扰或破坏的风险
- 重要数据被窃取、泄露、毁损的风险

断供风险

- 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
- 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

供应商合规风险

- 产品和服务提供者遵守中国法律、行政法规、部门规章情况

其它风险

- 其他可能危害关键信息基础设施安全和国家安全的因素

结合《公告》的规定，此次网络安全审查特别强调了“国家数据安全”，可见“重要数据被窃取、泄露、毁损的风险”是“滴滴出行”被采取网络安全审查的重要原因以及此次安全审查的重点。

https://www.sec.gov/news/press-release/2021-53

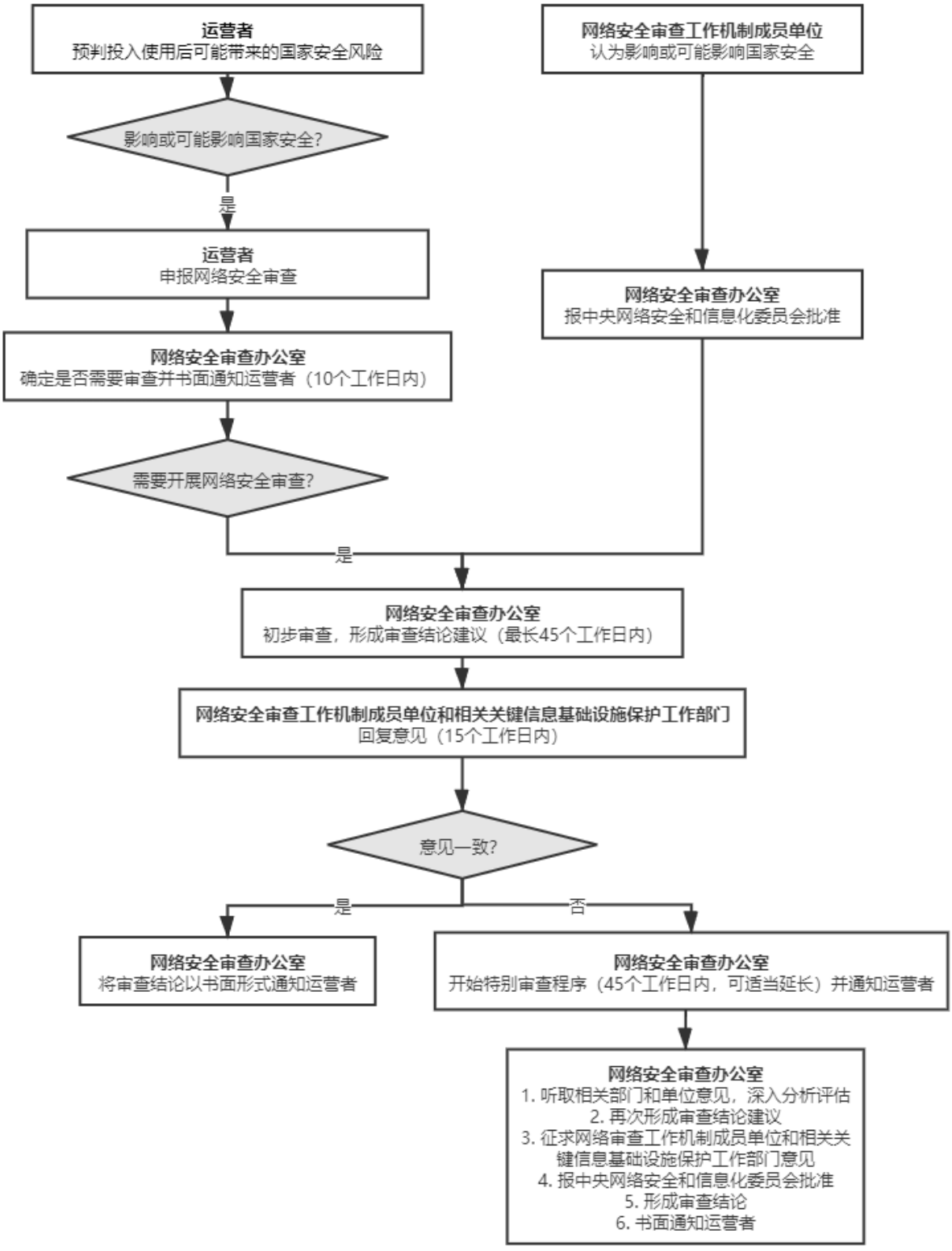
[6] 《外商投资准入特别管理措施(负面清单)(2020 年版)》《外国的组织或者个人来华测绘管理暂行办法》《关于加强自动驾驶地图生产测试与应用管理的通知》

参照网信办颁布的《个人信息和重要数据出境安全评估办法(征求意见稿)》以及《数据安全管理办法(征求意见稿)》，重要数据与国家安全、经济发展、社会公共利益、公共健康和安全密切相关，同时结合 2021 年 5 月网信办颁布的《汽车数据安全管理若干规定(征求意见稿)》，“滴滴出行”可能涉及了道路车辆类型数据，车辆流量数据，汽车充电网运行数据，包含人脸、声音、车牌的车外音视频数据等汽车数据处理活动中的重要数据，并且在处理该等数据的过程中，存在数据被窃取或泄露的风险。

此次网络安全审查强调“数据安全”，与《数据安全法》规定的“数据安全审查”相比，二者的审查对象有所不同，数据安全审查针对的是“影响或者可能影响国家安全的数据处理活动”。然而，尽管两种审查制度在法律依据、审查对象方面略有差别，但网络安全不可能脱离数据安全存在，网络安全产品和服务的本质是涉及数据的产品的和服务，针对网络安全产品和服务的网络安全审查也应当包括数据安全的内涵。此外，网络安全审查也并不仅局限于采购阶段，而是贯穿网络产品和服务的整个生命周期，包括事中事后要求 CIIO 督促提供方履行网络安全审查承诺，在这一过程中，也必然涉及数据安全。因此，CIIO 在网络安全审查中，不应忽视数据安全，否则将与《办法》背道而驰。

4. 网络安全审查的具体程序及后果?

网络安全审查的程序规定在《办法》第 5 条至第 15 条中，具体的审查程序如下图所示:



网络安全审查启动后，对于情况复杂的，CIIO 可能面临四个月甚至更长时间的审查。在此期间，对于依申请开展的网络安全审查，CIIO 可能无法在审查期间内签署网络产品与服务的供应合同；对于依职权开展的网络安全审查，CIIO 的日常业务可能受到相应影响，此次“滴滴出行”网络安全审查过程中，工信部已发布《关于下架“滴滴出行”App 的通报》，要求滴滴出行科技有限公司进行整改。

根据审查结果, 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。

如果"滴滴出行"确实存在与《办法》相关的违法情形, 可能面临严重的业务连续性问题, 直接负责人员和责任人员也会受到相应处罚。

5. 网络安全审查, 谁是下一家?

根据"网信中国"微信号于 7 月 5 日发布的消息, 为防范国家数据安全风险, 维护国家安全, 保障公共利益, 依据《国家安全法》《网安法》, 网络安全审查办公室按照《网络安全审查办法》, 对"运满满""货车帮""BOSS 直聘"实施网络安全审查。审查期间, 该等 APP 均停止新用户注册。可见"滴滴出行"被进行网络安全审查, 或许已经拉开了监管部门进行网络安全审查工作的序幕。

从《网安法》规定了网络安全审查制度, 到《办法》明确了网络安全审查的实施细则, 开展网络安全审查工作的法律依据和具体程序要求已经十分明确。CIIO, 可能被认定为 CIIO 的企业, 以及 CIIO 网络设备与产品的供应链企业, 不应抱着原先"等风来"的态度, 对落实网络安全审查制度抱有"观望"心态。相关的企业和机构应当即时有序地启动网络安全审查相关的合规工作, 包括:

作为采购方:

(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) 工作日; 而特别程序审查程序中, 需等待的时间为 115(70+45) 工作日甚至更长(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四个月以上的安全审查时间。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。

作为提供方:

(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。

另外，《数据安全法》确立了数据安全审查制度，亟待配套实施细则出台。借鉴此次“网络安全审查”第一案，我们或许可以预见到，在配套实施细则出台后不久，“数据安全审查”第一案也迟早会出现，网络安全审查与数据安全审查也会成为“相伴相生”的国家安全制度。我们建议企业宜尽早筹谋布局，对自身是否符合《网安法》《数据安全法》及相关网络、数据安全法律的规定进行评估、自查，并做好整改和应对措施。关于数据安全审查的相关解析详见《安全与发展并重——<数据安全法(草案)>要旨与解读》《能力越大，责任越大——数据分类分级制度评述》《网安法、个保法、数安法下的法律责任》等。

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

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	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	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