中倫
ZHONG LUN

《网络安全审查办法》修订
中国网络安全审查制度的演进与影响

中伦律师事务所 陈际红

——言中伦 行中虑——

主讲人简介

陈际红
权益合伙人

电话：+86 10 5957 2288

传真：+ 86 10 6568 1022

电邮: chenjihong@zhonglun.com

执业领域

TMT领域的法律事务，包括侵权诉讼，隐私与数据保护，计算机软件，不正当竞争，专利与商标申请，知识产权许可与交易，电子商务，电信，IT企业的投资与收购，互联网知识产权保护

个人荣誉

- 全国律师协会网络与高新技术委员会，副主任
- 国家知识产权局国家知识产权专家库，专家
- 国家知识产权战略办公室，入库知识产权战略专家
- 北京重点产业知识产权联盟，知识产权专家
- 中国互联网协会法治工作委员会，顾问

- 陈际红律师从1996年开始执业，为众多的国际企业提供了法律服务，并多次参与了与知识产权、电信、IT有关法律法规的研讨与立法工作，参与过的立法工作包括《网络安全法》、《关键信息基础设施保护条例（征求意见稿）》及网信办系列配套规章、《计算机软件保护条例》、《电子签名法》、《著作权法》等。新华社、人民日报等对他的研究与律师执业做过深入报道。

- 陈际红律师于2005年被法制日报及中国电子商务协会联合评为“2005IT法务人年度十佳”；2006年入选国家知识产权战略办公室评选的国家知识产权战略专家； 2011年入选英国Corporate INTL Magazines评选的“中国最佳50名律师”；2011年入选国家知识产权局评审的国家知识产权专家库；2013年陈律师被北京市律师协会授予“北京市十佳知识产权律师”的称号。2015年被ALB评选为中国最佳15名知识产权律师。于2016年，被Corporate INTL评选为中国年度最佳电信法律师；被Global Law Experts评选为（2016最佳中国电信法律师）Telecommunications Law - Lawyer of the Year in China – 2016；被MIP（Managing Intellectual Property）评选为“中国杰出知识产权律师”（IP Stars）。2019年，被《亚洲法律杂志》ALB评选为中国十五佳TMT律师，并再一次位列知产力和IPRdaily评选的“中国优秀知识产权律师榜TOP50榜单”。

提 纲

1. 如何理解滴滴事件的背景?
2. 什么原因推动了《网络安全审查办法》的修订?
3. 《网络安全审查办法》修订了什么?
4. 《网络安全审查办法》焦点十问
5. 企业应当如何合规应对?

第一部分 | 背景

滴滴网络安全审查及后续

滴滴于纽约证券交易所上市

2021年6月30日

2021年7月2日
网络安全审查办公室

为防范国家数据安全风险，维护国家安全，保障公共利益，**对“滴滴出行”实施网络安全审查**

“滴滴出行”App因存在严重违法违规收集使用个人信息问题而**被下架**

2021年7月4日
国家互联网信息办公室

2021年7月9日
国家互联网信息办公室

“滴滴企业版”App等25款滴滴系App因存在严重违法违规收集使用个人信息问题**被下架**

《网络安全审查办法（修订草案征求意见稿）》发布

2021年7月10日
国家互联网信息办公室

□ 滴滴网络安全审查及后续

网络安全审查办公室关于对“运满满”“货车帮”“BOSS直聘”启动网络安全审查的公告

网信中国 1周前

CAC 点击“网信中国”关注官方账号

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《中华人民共和国国家安全法》《中华人民共和国网络安全法》，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。为配合网络安全审查工作，防范风险扩大，审查期间“运满满”“货车帮”“BOSS直聘”停止新用户注册。

特此公告。

网络安全审查办公室

2021年7月5日

2021年已赴美上市的部分中概股（以融资规模排序）

公司名称	主要业务	上市时间	融资规模（亿美元）
滴滴出行*	网约车	6月30日	44.0
雾芯科技	电子烟	1月22日	16.1
满帮*	数字货运	6月22日	14.9
图森未来	自动驾驶	4月15日	13.5
涂鸦智能	物联网平台	3月18日	9.2
BOSS直聘*	在线招聘	6月11日	9.1
知乎	在线问答	3月26日	5.2
水滴	保险科技	5月7日	3.6

*被中国国家网信办实施网络安全审查　　联合早报整理 zaobao

□ 滴滴网络安全审查及后续

2009年，《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》：在境外发行证券与上市过程中，证券公司、证券服务机构在境内形成的工作底稿等档案应当存放在境内。

财政部2015《会计师事务所从事中国内地企业境外上市审计业务暂行规定》：中国内地公司依法委托境外会计师事务所审计的，其在中国境内形成的底稿应当存放在境内。

五、进一步加强跨境监管执法司法协作

（十九）加强跨境监管合作。**完善数据安全、跨境数据流动、涉密信息管理等相关法律法规。**抓紧修订关于加强在境外发行证券与上市相关保密和档案管理工作的规定，**压实境外上市公司信息安全主体责任。加强跨境信息提供机制与流程的规范管理。坚持依法和对等原则，进一步深化跨境审计监管合作。**探索加强国际证券执法协作的有效路径和方式，积极参与国际金融治理，推动建立打击跨境证券违法犯罪行为的执法联盟。

- 2020年12月2日，美国国会通过了《外国公司问责法案》（Holding Foreign Company Accountable Act，以下简称“《问责法案》”）。特朗普已于12月18日签署了该法案。
- 《问责法案》是对2002年实施的Sarbanes-Oxley (SOX) Act的进一步补充。
- 《问责法案》在此基础上新增了对外国上市公司更严格的信息披露和审计要求，还加入了专门针对中国上市公司的额外披露义务。

口 什么原因推动了《网络安全审查办法》的修订?

《数据安全法》将于9月10日实施

《数据安全法》第二十四条：国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。依法作出的安全审查决定为最终决定。

境外上市的信息披露义务

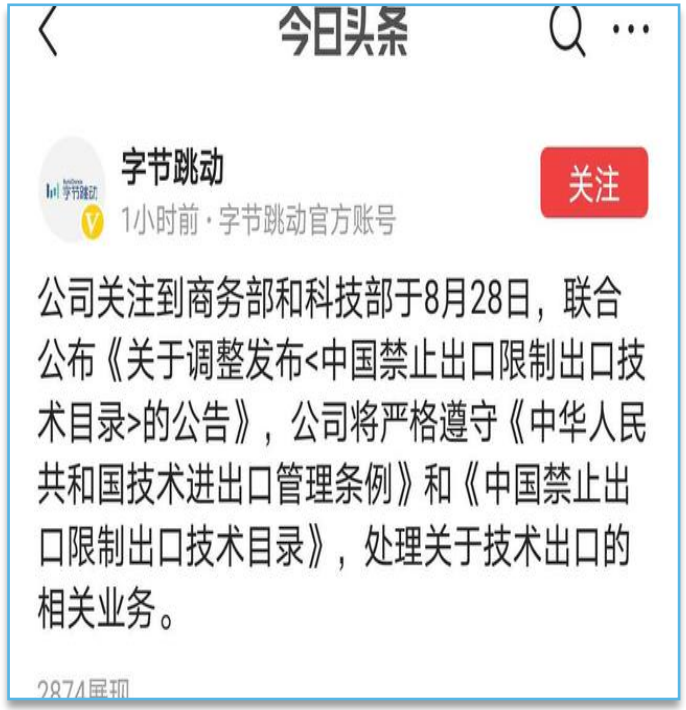
在境外上市，意味着上市公司需要进行持续性的信息披露。
涉及数据的跨境传输和披露。

“长臂管辖权”

基本法理依据是“最低限度联系理论”和所谓“效果原则”。
在美国上市明显地建立了和美国法的链接点。

制裁反制裁

2020年8 月，美国总统特朗普签署行政令，禁止任何美国个人或实体与抖音海外版(TikTok)、微信（WeChat）及其中国母公司进行任何交易。
6月10日，全国人大通过《中华人民共和国反外国制裁法》。



根据《中华人民共和国技术进出口管理条例》，凡是涉及向境外转移技术，无论是采用贸易还是投资或是其他方式，均要严格遵守《中华人民共和国技术进出口管理条例》的规定。

第二部分 | 主要修订内容

修订了什么？ - 《数据安全法》

- 《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网络信息技术产品和服务，以及其他重大事项和活动，进行国家安全审查。
- 《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，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”
- 《数据安全法》第二十四条：国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。依法作出的安全审查决定为最终决定。

2017.6.1
《网络产品和服务安全审查办法（试行）》

提高**网络产品和服务**安全可控水平，防范网络安全风险，维护国家安全

2019.5.24
《网络安全审查办法（征求意见稿）》

提高**关键信息基础设施**安全可控水平，维护国家安全

2020.6.1
《网络安全审查办法》

确保**关键信息基础设施供应链**安全，维护国家安全

2021.7.10
《网络安全审查办法（修订草案征求意见稿）》

确保**关键信息基础设施供应链、数据处理活动**安全，维护国家安全

➢ **网络安全审查逐步聚焦：**

- 网络产品和服务安全可控
- CII安全可控
- 确保CII供应链安全
- + 数据处理活动安全

修订了什么？ - 涵盖数据处理活动

义务主体：运营者

关键信息基础设施运营者

数据处理者

监管行为

采购网络产品和服务

开展数据处理活动

国外上市

修订了什么？ - 触发网络安全审查的情形

CIIO采购。CIIO采购网络产品和服务，应当预判国家安全风险。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。 由网络安全审查办公室确定是否需要审查。

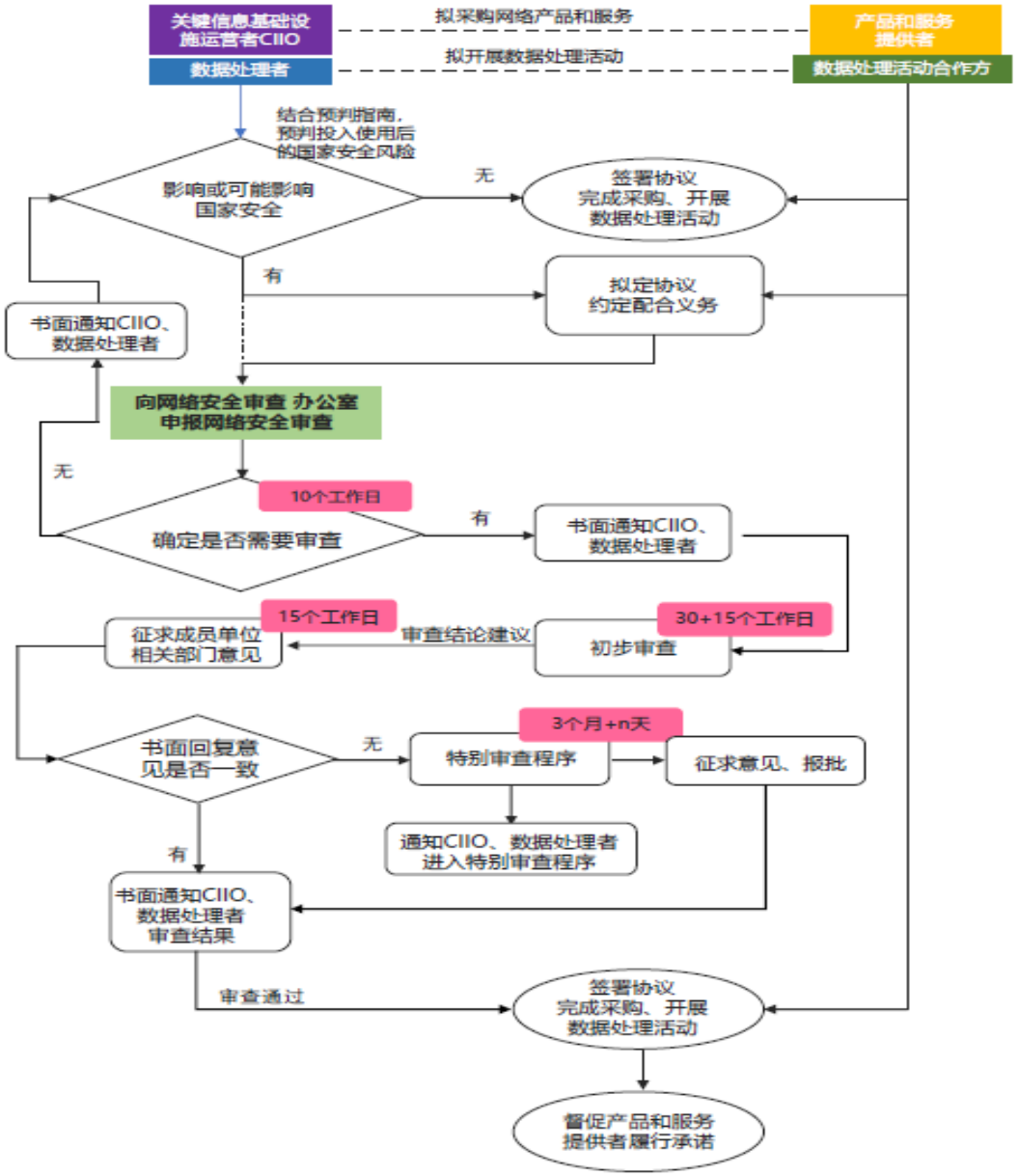
国外上市。掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

依职权启动。 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。

数据处理活动。数据处理者开展数据处理活动，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。

修订了什么？ - 更新程序

- ✓ 特别审查程序：时间由45天延长至3个月。
- ✓ 一般情形下的网络安全审查在60个工作日（45日+15日）内完成，
- ✓ 特别审查程序，审查周期可能为5个月（45日+15日+3个月）甚至更长。
- ✓ 网络安全审查办公室要求提交补充材料的时间不计入审查时间。

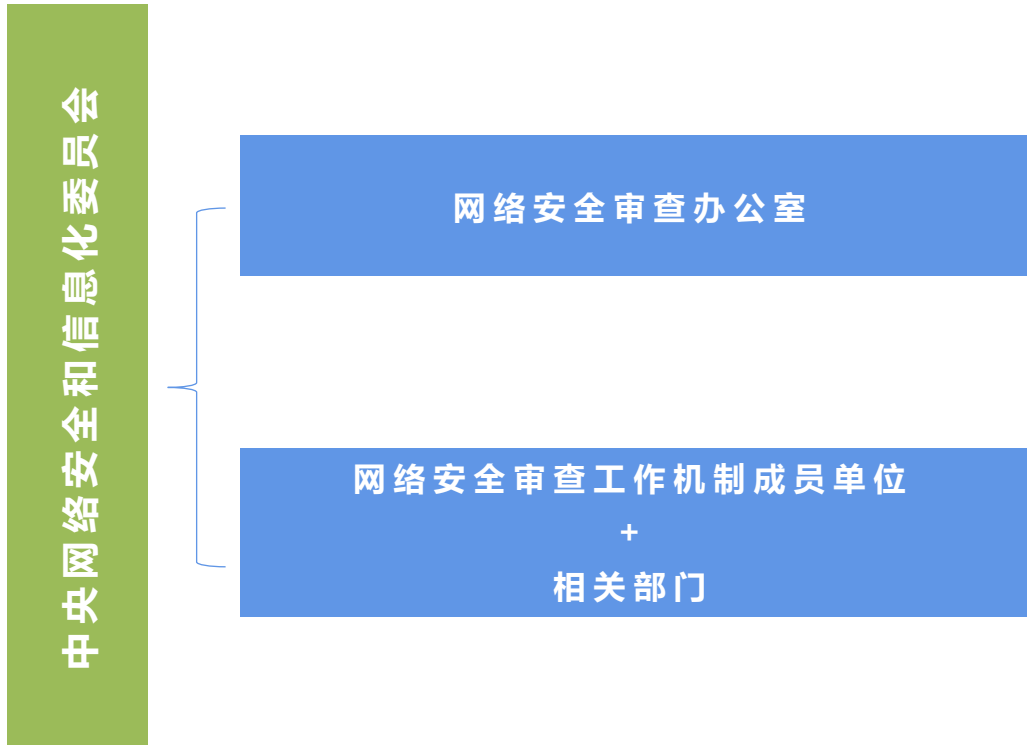


口修订了什么？ - 证监会

审查工作机构包含三类

由中央网络安全和信息化委员会统一领导网络安全审查工作，包括国家互联网信息办公室在内的12个国务院组成部门和直属机构共同建立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，负责制定规范，组织审查，具体工作委托中国网络安全审查技术与认证中心承担。

➢ **三类审查机构**



➢ **13个组成部门**

口修订了什么？ - 上市申报门槛：百万个人信息

第六条 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。

- **上市如何理解？**

包括境内公司在国外的IPO、SPAC、RTO，还可能包括已上市公司的股票增发以及发债等一系列融资行为。

- **“掌握”如何理解？**

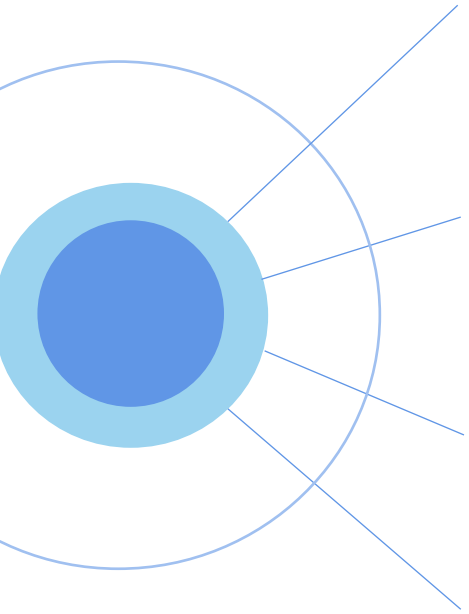
《个人信息安全规范》中的“控制”
《个人信息保护法（草案）》以及《数据安全法》中的“处理”

- **云计算服务会成为申报主体吗？**

- **国外 v. 境外，香港H股包括吗？**

- **如何计算100万？**

口修订了什么？ - 审核评估因素



- **强调产品和服务使用后对CII产生的风险**
- **强调重要数据相关风险**
- **强调供应链中断对业务连续性的危害风险**
- **要求确保产品和服务来源的多样性、供应渠道的可靠性**

第十条 网络安全审查重点评估采购活动、数据处理活动以及国外上市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；↵

（六）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；↵

（七）其他可能危害关键信息基础设施安全和国家数据安全的因素↵

第三部分｜　焦点十问

□ 争议或焦点问题

1. 网络安全审查会成为一个普遍执法的制度吗？ 执法频率会增加吗?
2. 已经上市的企业需要启动网络安全审查吗?
3. 这项制度会影响TMT企业的估值吗?
4. VIE架构还能继续吗?
5. 香港上市是否是例外?需要进行网络安全审查吗？ 会成为境外上市首选地吗?
6. 网络安全审查不通过的后果是什么？可以救济吗?
7. 如果确定国外上市，企业要做什么准备?
8. 100万个人信息如何计算?
9. 什么是CII和CIIO，与网络安全审查的关系是什么?
10. 什么是核心数据和重要数据，如网络安全审查的关系是什么?

□ CII和CIIO的识别与认定

- **2016《网络安全法》：**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实施重点保护。

- **2017《关键信息基础设施安全保护条例》（征求意见稿）：** 关键信息基础设施是指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、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能会严重危害国家安全、国计民生、公共利益的网络设施、信息系统等。

- **2016年，中央网信办制定《关键信息基础设施确定指南（试行）》**、《国家网络安全检查操作指南》。2016年6月，中央网信办组建国家关键信息基础设施网络安全检查办公室，组织开展了第一次全国范围内的CII摸底检查工作。
- **2020年公安部《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》**：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、国防科技工业等重要行业和领域的主管、监管部门应制定本行业、本领域关键信息基础设施认定规则并报公安部备案。 同时应将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纳入关键信息基础设施。

- **标准制定：**《信息安全技术 关键信息基础设施边界确定方法》、《信息安全技术 关键信息基础设施网络安全保护基本要求》等标准正在研究制定

CII认定与边界识别

关键信息基础设施的认定方法

1

第一步：确定关键业务

包括但不限于能源、金融、交通、水利、医疗卫生、环境保护、工业制造、市政、电信与互联网、广播电视、教育、新闻网站、商业平台、政府部门

2

第二步：确定信息系统或工业控制系统

根据关键业务逐一梳理支撑关键业务运行或与关键业务相关的信息系统或工业控制系统

3

第三步：认定CII

根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施

关键信息基础设施的边界识别

1

第一步：确定重要行业和领域

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、国防科技工业等

2

第二步：确定关键业务及运营者

识别重要行业和领域内影响国家安全、国计民生、公共利益的关键核心业务及其运营者

3

第三步：确定CII边界

识别关键业务持续、稳定运行所必须的网络设施、信息系统

□ 核心数据、重要数据

1. 什么是重要数据

《信息安全技术 重要数据识别指南》标准的制定还在进行。 参照《重要数据识别指南》草案，重要数据目前可以理解为，我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能对**国家安全、国家经济和金融安全、社会公共利益、个人合法权益**等造成相关严重后果的数据。

2. 重要数据目录怎么制定?

重要数据目录由国家数据安全工作协调机制统筹协调有关部门制定，形成国家层面的重要数据目录；而各地区、各部门将确定本地区、本部门以及相关行业、领域的重要数据具体目录。

3. 什么是核心数据?

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。

要上市，法律上做什么?

- 政策解读和跟进，准确理解要点、精神和适用，确定适用以及策略，方案设计，如果需要跟监管访谈安排。
- 协助公司按照进行网络安全审查所需的合规自查，并完成整改，出具自查报告。
- 撰写网络安全审查申请书和所需报告 申报文件确定
- 协助公司通过网络安全审查（包括协助公司补充材料，解答问题等）进入程序，协助进行应对
- 如果网络安全审查过程中提出整改要求或增强措施要求，协助公司完成整改或措施的落地。 如果审查附条件通过或者不通过，法律联合技术提供商提供落地实施。

□ 网络产品和服务的范围

➢ 审查范围

- 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
- 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

- +重要通信产品

《网络安全审查办法》第二十条

附件

网络关键设备和网络安全专用产品目录(第一批)

	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量(双向)≥12Tbps 整系统路由表容量≥55 万条
	2. 交换机	整系统吞吐量(双向)≥30Tbps 整系统包转发率≥10Gpps
	3. 服务器(机架式)	CPU 数量≥8 个 单 CPU 内核数≥14 个 内存容量≥256GB
	4. 可编程逻辑控制器(PLC 设备)	控制器指令执行时间≤0.08 微秒
网络安全专用产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1 小时
	6. 防火墙(硬件)	整机吞吐量≥80Gbps 最大并发连接数≥300 万 每秒新建连接数≥25 万
	7. WEB 应用防火墙(WAF)	整机应用吞吐量≥6Gbps 最大 HTTP 并发连接数≥200 万
	8. 入侵检测系统(IDS)	满检速率≥15Gbps 最大并发连接数≥500 万
	9. 入侵防御系统(IPS)	满检速率≥20Gbps 最大并发连接数≥500 万
	10. 安全隔离与信息交换产品(网闸)	吞吐量≥1Gbps 系统延时≤5ms
	11. 反垃圾邮件产品	连接处理速率(连接/秒)>100 平均延迟时间<100ms
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5 万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥60 个
	14. 安全数据库系统	TPC-E tpsE(每秒可交易数量)≥4500 个
	15. 网站恢复产品(硬件)	恢复时间≤2ms 站点的最长路径≥10 级

抄送:中央国家机关有关部门。

国家互联网信息办公室秘书局　　2017 年 6 月 1 日印发

共印 200 份

— 4 —

➢ 一般的网络产品和服务

《网络安全法》第二十二条

➢ 网络关键设备和网络安全专用产品

《网络安全法》第二十三条

《网络关键设备和网络安全专用产品目录》》

➢ 计算机信息系统安全专用产品

《计算机信息系统安全专用产品检测和销售许可证管理办法》、《信息安全等级保护管理办法》

➢ 密码产品

《密码法》第二十六条

第四部分 | 合规应对

企业具体合规应对

数据资产和数据业务场景盘点

- 结合自身业务进行数据识别、梳理和盘点工作，对于数据资产的情况进行充分了解，对于可能涉及重要数据、国家核心数据、处理用户数量到达百万级别以上的产品和业务线进行重点关注，及时开展合规自查和整改工作。

数据分类分级+保护措施

- 建立内部的数据分类分级制度并实行对应的保护措施，密切关注核心数据和重要数据的认定标准和指南。在相关识别指引出台前，建议依据定义做初步识别，如有必要进行监管沟通，积极管理风险。

CII识别与认定

- 持续关注CII的认定标准，评估自身适用的义务项。如构成CIIO的情况下，应当建立和完善自身的招采评估制度以及网络安全审查预判制度，初步判断是否会影响国家安全，并配合后续的审查。

□ 企业具体合规应对

上市策略

- 审慎选择上市地点，全面评估数据风险和监管风险。在确定国外上市的情况下，充分考虑网络安全审查的可能性，与监管机构保持沟通，配合国外监管机构的信息披露要求时严格遵守国内法律法规要求。如果必要，事先获得国内主管部门的批准，履行相应评估程序。

持续合规

- 企业运营过程中持续保持数据处理的合规性，完善企业内部的个人信息保护制度及数据安全制度，建立数据安全影响评估制度，根据法律要求和行业良好实践及时审视自身的合规状况，落实合规义务。

谢谢！

——言中伦 行中虑——