汉坤法律评述
漢坤律師事務所
融贯中西 · 务实创新
2017 年 5 月 5 日

汉坤网络安全和数据合规系列之四：网安审查，大幕开启！

唐志华 | 朱敏

2017 年 5 月 2 日，国家互联网信息办公室（“**网信办**”）发布了《网络产品和服务安全审查办法（试行）》（“**《审查办法》**”），并将于 2017 年 6 月 1 日起生效。这是《网络安全法》于 2016 年 11 月 7 日发布之后又一项新出台的配套措施，旨在落实《网络安全法》第三十五条所规定的安全审查要求。

一、 变化对比

相比于网信办于 2017 年 2 月 4 日发布的《网络产品和服务安全审查办法（征求意见稿）》（“**征求意见稿**”），《审查办法》做了一些明显的调整，主要有：

1. 在全文中删除了“公共利益”的范围界定。我们理解，“公共利益”的表述太过模糊和宽泛，使网络安全审查具备了无远弗届的适用边界。因此，该项删除不仅使《审查办法》的规制范围更加明确，也体现了国家在网络安全审查上的关切重点所在；

2. 网络安全审查内容更加明确。《审查办法》在强调安全性和可控性的要求下，明确了审查内容包括静态审查（产品和服务自身的安全风险）和动态审查（产品及关键部位的供应链安全风险，即生产、测试、交付和技术支持的全过程）；

3. 再次重申了重点行业和领域。与《网络安全法》第三十一条关于关键信息基础设施的规定相呼应，《审查办法》再次重申安全审查所重点关注的领域，即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。值得一提的是，《审查办法》删除了《征求意见稿》中“党政机关”的描述，我们理解这是因为“党政机关”性质特殊，本身也已有相应的安全审查机制，从而无需在《审查办法》中予以列明。

二、 主要内容

正式发布的《审查办法》有如下一些值得关注的重点内容：

1. 不设准入审批，强调事中事后监管

纵观《审查办法》全文，新规并没有对网络产品和服务提供者的市场准入设定新的行政许可事项，而只是强调“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应当经过网络安全审查”

（第二条），且“坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品和服务及其供应链进行网络安全审查”（第三条），明显属于事中事后的过程监管。

2. “安全“和“可控”的审查标准

从《网络安全法》立法伊始，“安全”和“可控”就是立法者和监管者语境里使用最为频繁的两个措辞，也是指导《网络安全法》立法和执法的基本原则。这一点也在此次《审查办法》的出台中再次得到了印证。《审查办法》第四条规定，安全审查的重点是产品和服务的安全性与可控性，具体包括：（一）产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；（二）产品及关键部件的供应链安全风险；（三）产品和服务提供者利用非法收集、存储、处理、使用用户相关信息的风险；（四）产品和服务提供者损害网络安全和用户利益的风险；以及（五）其他可能危害国家安全的风险。

其中，第（一）和（二）项属于风险防御能力评估条款，第（三）和（四）项属于主动侵害行为禁止条款，如此规定，可谓正反兼顾。但总体而言，这些内容还是原则性表述，若没有进一步说明，实践操作中很难预测审查的范围和尺度，相关审查主体自由裁量的空间较大。

3. 多方主体参与，力求程序正当

安全审查的程序设计是本次《审查办法》着力最多的一个部分，第五条至第十条均与此相关。而这些条款设计，则在很大程度上彰显了现代行政程序法意义下的行政参与和程序正当。

例如，从参与主体上而言，本次《审查办法》覆盖了网络安全审查委员会（新设机构）、网络安全审查办公室、网络安全审查专家委员会、第三方机构、全国性行业协会、用户、行业主管部门和关键信息基础设施保护工作部门。从程序正当上而言，则设置了专家参与、社会参与和公众参与等各种程序机制。

但很显然，有关安全审查的最终决定还是要由政府监管机构做出。因此，在一定程度上，与当下提倡的“小政府、大社会”的简政放权思路不同，在网络安全领域，立法者还是希望体现更多的政府意志。

4. 监管部门主导启动程序

《审查办法》也明确了安全审查的启动程序。第八条规定：网络安全审查办公室根据国家有关部门要求、全国性行业协会建议、用户反映启动网络安全审查。第九条规定：金融、电信、能源等重点行业主管部门，根据国家网络安全审查工作要求，组织开展本行业、本领域网络产品和服务安全审查工作。

与征求意见稿相比，《审查办法》删除了“企业申请”的启动选项。因此，在安全审查的启动机制上，企业已经没有了主动权，在必要的情况下最多只能通过行业协会等间接渠道推进。这一点，也与上面所述的政府意志色彩相吻合，政府倾向于采取积极行政和主动监管的路径。

5. 安全评估报告：网安审查的“黑名单”制度？

《审查办法》第十三条规定，网络安全审查办公室不定期发布网络产品和服务安全评估报告。虽然没有明确报告的具体形式和内容，但根据我们跟踪相关立法进程中所获知的信息，安全评估报告不

仅会公布符合安全审查要求的网络产品和服务及其提供者的信息，也会公布未通过安全审查的网络产品和服务名单，由此形成“白名单”＋“黑名单”的信息公开制度，并以此对行业监管施加影响和形成导向。

此外，网信办相关负责人曾表示，网络审查将对国内外企业和产品平等对待，不针对特定国家地区的产品和服务，不会限制国外产品进入中国市场。但鉴于网络安全审查关注的重点是“国家安全”，对于境外企业或者境内的外商投资企业及其所提供的产品和服务是否会在无形之中形成一定的市场准入壁垒，仍有待观察。

三、 对企业的建议

网络产品与服务的安全审查严格来讲之前并非是一片空白。一则国家针对特定的行业、产品和服务已有一些既定的质量标准、行业准入以及企业资质等的监管要求；二则很多企业本身也会有自己的产品安全要求，某些行业也制定了行业标准。但就全国层面而言，之前并没有专门的制度性文件来确定统一的安全审查制度和标准。此次《审查办法》的出台，可以说开启了国家主导层面的网安审查的大幕。

就目前的文件内容而言，《审查办法》只是网络产品和服务安全审查的一个原则性和纲领性文件，很多内容仍有待细化和明确，例如网络安全审查委员会和专家委员会的机构设置、第三方机构的认定、影响国家安全的评估标准以及相应的审查程序和工作细则等等。

虽然相关细则还没有出台，但相关罚则实际已经到位。按照《网络安全法》第六十五条规定，关键信息基础设施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。如果违法情节严重而被监管机构顶格处罚的话，处罚责任不可谓不重。

因此，我们仍建议网络产品和服务的运营者和提供者，尤其是重点领域和行业的关键信息基础设施运营者，应当对照安全性和可控性的标准和要求，对采购的或向他人提供的网络产品和服务进行内部安全审查，及时改进，同时与行业协会和政府监管部门保持良好沟通，并持续关注相关领域政策的后续发展。

汉坤网络安全和数据合规系列：

之一：健康医疗大数据领域的政策和法律问题

之二：《网络安全法》简评

之三：数据出境不再任性

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤**唐志华律师（+8621-6080 0905; david.tang@hankunlaw.com**）或**朱敏律师（+8621-6080 0955; min.zhu@hankunlaw.com**）联系。