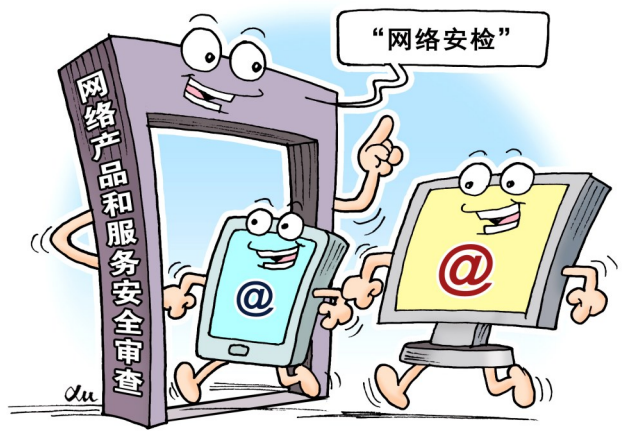
帮你预习“网络安检”须知

——聚焦《网络产品和服务安全审查办法（征求意见稿）》

国家互联网信息办公室近日公布的《网络产品和服务安全审查办法（征求意见稿）》提出，我国将成立网络安全审查委员会，统一组织网络安全审查工作等。“网络安检”有哪些须知项？新华社记者采访了国家网信办和网络安全领域专家。



焦点一：谁来审查，是什么性质的审查？

【意见稿】国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，协调网络安全审查相关重要问题。

【解读】国家网信办相关负责人表示，中国借鉴国外做法，建立网络安全审查制度。网络安全审查委员会聘请相关专家组成网络安全审查专家委员会，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估。网络安全审查不是行政审批，是对重要网络产品和服务采取的事中、事后监管，坚持实验室检测、现场检查、在线监测、背景调查相结合的原则。

焦点二：哪些产品和服务需审查？

【意见稿】关系国家安全和公共利益的信息系统使用的重要网络产品和服务，应当经过网络安全审查。

【解读】国家网信办相关负责人介绍，并非所有网络产品和服务都需要审查，是有条件的。而且，重点审查的是网络产品和服务的安全性、可控性。判定是否影响国家安全和公共利益，主要看产品和服务使用后，是否会危害国家政权和主权安全，是否会危害广大人民群众利益，是否会影响国家经济可持续发展及国家其他重大利益。

焦点三：党政部门所用产品都要审查？

【意见稿】党政部门及重点行业优先采购通过审查的网络产品和服务，不得采购审查未通过的网络产品和服务。

【解读】中国信息安全研究院副院长左晓栋说，这个规定的意思是，如果某个网络产品和服务可能会影响国家安全，在进行安全审查后没能通过审查，被列入“黑名单”后不能采购，并不是说党政部门及重点行业采购的所有网络产品和服务都要进行审查。

焦点四：是在搞贸易保护壁垒吗？

【意见稿】关键信息基础设施运营者采购的网络产品和服务，可能影响国家安全的，应当经过网络安全审查。

【解读】国家网信办相关负责人介绍，网络安全审查制度的实施是企业证明产品安全性，提高用户对产品信心的机会。网络安全审查不但不会对国外产品进入中国市场造成障碍，反而会因审查制度的实施提高用户对产品安全性的信心，促进企业产品市场的扩大。网络安全审查将对国内外企业和产品平等对待，不针对特定国家和地区的产品和服务，不会限制国外产品进入中国市场。

焦点五：网络安全审查和网民有什么关系？

【意见稿】重点审查网络产品和服务的安全性、可控性，主要包括：产品和服务被非法控制、干扰和中断运行的风险；产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、利用用户相关信息的风险；产品和服务提供者利用用户对产品和服务的依赖，实施不正当竞争或损害用户利益的风险等。

【解读】国家网信办相关负责人介绍，重点审查网络产品和服务的安全性、可控性，产品和服务提供者不得利用提供产品和服务的便利条件非法获取用户的信息，不能损害用户对自己信息的自主权、支配权；不得非法控制、操纵用户的系统或设备，用户自己的系统要用户自己控制；不得利用广大用户对产品和服务的依赖搞不正当竞争，谋取不正当利益，比如停止必要的安全服务、搞垄断经营等。目的是维护用户信息安全，维护国家安全和广大人民群众的合法权益。

焦点六：审查如何才会启动？

【意见稿】根据国家有关部门要求、全国性行业协会建议、市场反映和企业申请等，网络安全审查办公室组织第三方机构、专家对网络产品和服务进行网络安全审查。

【解读】国家网信办相关负责人介绍，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、市场反映和企业申请启动网络安全审查。同时，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。

左晓栋解释，比如某网络产品和服务，全国性行业协会经过研究认为这款产品和服务存在巨大网络安全漏洞，可能影响国家安全，就可以向审查委员会反映这个问题，审查委员会认为这种情况可能存在，就可以对该产品和服务在特定领域使用时进行安全审查。

[相关链接]

为了咱们的网络安全，国家放过哪些大招？

网络空间正全面改变人们的生产生活方式，但安全问题不容忽视。除了正在征求意见的“网络产品和服务安全审查办法”外，我国近年来出台不少法律法规和文件，放出大招，打造安全稳定的网络空间。

国家安全法：建设网络与信息安全保障体系

2015年7月通过的国家安全法明确规定：国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

网络安全法：网络领域的基础性法律

2016年11月通过的网络安全法是我国网络领域的基础性法律，明确加强对个人信息保护，打击网络诈骗。该法将于今年6月1日起施行。

针对个人信息泄露问题，网络安全法规定：网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；网络运营者不得泄露、篡改、毁损其收集的个人信息；任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

针对网络诈骗多发态势，网络安全法规定，任何个人和组织不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

《国家网络空间安全战略》：保障网络空间安全的“防火墙”

2016年12月，国家互联网信息办公室发布《国家网络空间安全战略》。这一指导国家网络安全工作的纲领性文件，将为保障我国网络空间安全铸造一道“防火墙”。

战略提出，健全网络安全法律法规体系，加快对现行法律的修订和解释，使之适用于网络空间；加快构建法律规范、行政监管、行业自律、技术保障、公众监督、社会教育相结合的网络治理体系，鼓励社会组织等参与网络治理，鼓励网民举报网络违法行为和不良信息。

同时，我国将采取包括经济、政治、科技、军事等一切措施，坚定不移地维护我国网络空间主权。加强网络反恐、反间谍、反窃密能力建设，严厉打击网络恐怖和网络间谍活动，严厉打击贩枪贩毒、传播淫秽色情、黑客攻击等违法犯罪行为。

（据新华社）