网络安全审查办法

发布日期：2022-01-04 来源：中国网信网

第一条 为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，根据《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》，制定本办法。

第二条 关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。

前款规定的关键信息基础设施运营者、网络平台运营者统称为当事人。

第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。

第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局建立国家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，负责制定网络安全审查相关制度规范，组织网络安全审查。

第五条 关键信息基础设施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。

关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。

第六条 对于申报网络安全审查的采购活动，关键信息基础设施运营者应当通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括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，无正当理由不中断产品供应或者必要的技术支持服务等。

第七条 掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

第八条 当事人申报网络安全审查，应当提交以下材料：

（一）申报书；

（二）关于影响或者可能影响国家安全的分析报告；

（三）采购文件、协议、拟签订的合同或者拟提交的首次公开募股（IPO）

等上市申请文件；

（四）网络安全审查工作需要的其他材料。

第九条 网络安全审查办公室应当自收到符合本办法第八条规定的审查申报材料起10个工作日内，确定是否需要审查并书面通知当事人。

第十条 网络安全审查重点评估相关对象或者情形的以下国家安全风险因素：

（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、遭受干扰或者破坏的风险；

（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、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险；

（六）上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险；

（七）其他可能危害关键信息基础设施安全、网络安全和数据安全的因素。

第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向当事人发出书面通知之日起30个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关部门征求意见；情况复杂的，可以延长15个工作日。

第十二条 网络安全审查工作机制成员单位和相关部门应当自收到审查结论建议之日起15个工作日内书面回复意见。

网络安全审查工作机制成员单位、相关部门意见一致的，网络安全审查办公室以书面形式将审查结论通知当事人；意见不一致的，按照特别审查程序处理，并通知当事人。

第十三条 按照特别审查程序处理的，网络安全审查办公室应当听取相关单位和部门意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知当事人。

第十四条 特别审查程序一般应当在90个工作日内完成，情况复杂的可以延长。

第十五条 网络安全审查办公室要求提供补充材料的，当事人、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。

第十六条 网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务以及数据处理活动，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。

为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。

第十七条 参与网络安全审查的相关机构和人员应当严格保护知识产权，对在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或者用于审查以外的目的。

第十八条 当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知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。

第十九条 当事人应当督促产品和服务提供者履行网络安全审查中作出的承诺。

网络安全审查办公室通过接受举报等形式加强事前事中事后监督。

第二十条 当事人违反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》的规定处理。

第二十一条 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、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、网络安全和数据安全有重要影响的网络产品和服务。

第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。

国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。

第二十三条 本办法自 2022 年 2 月 15 日起施行。2020 年 4 月 13 日公布的《网络安全审查办法》（国家互联网信息办公室、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、国家密码管理局令第 6 号）同时废止。