**网络安全审查办法**

（征求意见稿）

**第一条** 为提高关键信息基础设施安全可控水平，维护国家安全，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》等法律法规，制定本办法。

**第二条** 关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，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。法律、行政法规另有规定的，依照其规定。

**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、增强公正透明与保护知识产权相统一，坚持事前审查与持续监管、企业承诺与社会监督相结合，从产品和服务安全性、可能对国家安全带来的风险隐患等方面进行综合分析评判。

**第四条** 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。

**第五条** 国家互联网信息办公室会同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、商务部、财政部、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，负责组织制定网络安全审查相关制度规定和工作程序、组织网络安全审查、监督审查决定的实施。

**第六条** 运营者采购网络产品和服务时，应预判产品和服务上线运行后带来的潜在安全风险，形成安全风险报告。可能导致以下情况的，应当向网络安全审查办公室申报网络安全审查：

    （一）关键信息基础设施整体停止运转或主要功能不能正常运行；

    （二）大量个人信息和重要数据泄露、丢失、毁损或出境；

    （三）关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁；

    （四）其他严重危害关键信息基础设施安全的风险隐患。

**第七条** 对于申报网络安全审查的采购活动，运营者应通过采购文件、合同或其他有约束力的手段要求产品和服务提供者配合网络安全审查，并与产品和服务提供者约定网络安全审查通过后合同方可生效。

**第八条** 运营者申报网络安全审查时，应当提交以下材料：

    （一）申报书；

    （二）本办法第六条中的安全风险报告；

    （三）采购合同、协议等；

    （四）网络安全审查办公室要求的其他材料。

**第九条** 网络安全审查办公室受理网络安全审查后，应在30个工作日内完成初步审查，情况复杂的可延长15个工作日。

**第十条** 网络安全审查重点评估采购活动可能带来的国家安全风险，主要考虑以下因素：

    （一）对关键信息基础设施持续安全稳定运行的影响，包括关键信息基础设施被控制、被干扰和业务连续性被损害的可能性；

    （二）导致大量个人信息和重要数据泄露、丢失、毁损、出境等的可能性；

    （三）产品和服务的可控性、透明性以及供应链安全，包括因为政治、外交、贸易等非技术因素导致产品和服务供应中断的可能性；

    （四）对国防军工、关键信息基础设施相关技术和产业的影响；

    （五）产品和服务提供者遵守国家法律与行政法规情况，以及承诺承担的责任和义务；

    （六）产品和服务提供者受外国政府资助、控制等情况；

    （七）其他可能危害关键信息基础设施安全和国家安全的因素。

**第十一条** 网络安全审查办公室完成初步审查后，应形成审查结论建议，并送网络安全审查工作机制成员单位征求意见。审查结论建议包括通过审查、附条件通过审查、未通过审查三种情况。

    网络安全审查工作机制成员单位应在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意见一致的，网络安全审查办公室以书面形式将审查结论反馈运营者；意见不一致的，进入特别审查程序并通知运营者。

**第十二条** 进入特别审查程序的，网络安全审查办公室应进一步听取相关部门、专业机构、专家意见，进行深入分析评估，形成审查结论建议，征求网络安全审查工作机制成员单位意见后，按程序报中央网络安全和信息化委员会批准。

**第十三条** 特别审查原则上应在45个工作日内完成，情况复杂的可以延长。

**第十四条** 网络安全审查办公室要求提供补充材料等，运营者应予以配合。审查时间从提交补充材料之日起计算。

    运营者应对所提供材料的真实性负责。在审查过程中拒绝按要求提供材料或故意提供虚假材料的，按未通过安全审查处理。

**第十五条** 参与网络安全审查的人员对审查工作中获悉的信息等承担保密义务，不得用于审查以外的目的。

**第十六条** 运营者加强安全管理，督促产品和服务提供者认真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抽查、接受举报等形式加强事中事后监管。

**第十七条** 运营者违反本办法规定的，依照《中华人民共和国网络安全法》第六十五条的规定处理。

**第十八条** 本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。

    安全可控是指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数据、非法控制和操纵用户设备，不得利用用户对产品和服务的依赖性牟取不正当利益或者迫使用户更新换代等。

**第十九条** 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采购活动、信息技术服务活动，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，依照本办法进行审查。

**第二十条** 涉及国家秘密信息的，依照国家有关保密规定执行。

**第二十一条** 本办法自 年 月 日起实施，《网络产品和服务安全审查办法（试行）》同时废止。