君合研究简讯

JUNHE

2020 年 9 月 29 日

信息保护和网络安全法律热点问题

公安部发布网络安全等级保护和关键信息基础设施安全保护制度实践指导

2020 年 7 月 22 日，公安部向中央和国家机关各部委，国务院各直属机构、办事机构、事业单位，各中央企业下发了关于印送《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》的函（以下简称“**《指导意见》**”），以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为基础，保护关键信息基础设施、重要网络和数据安全为重点，构建国家网络安全综合防控体系。2020 年 9 月 22 日此《指导意见》公开发布[1]。

一、网络安全等级保护制度执法深入化、常态化

《指导意见》总结了现有法规及实践中的网络安全等级保护的要求，强调应深入推进网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作。

定级备案要求。网络运营者应全面梳理本单位各类网络，特别是云计算、物联网、新型互联网、大数据、智能制造等新技术应用的基本情况，并根据网络的功能、服务范围、服务对象和处理数据等情况，科学确定网络的安全保护等级，对第二级以上的网络，依法向公安机关备案并向行业主管部门报备。

测评要求。第三级以上网络运营者应委托符合国家有关规定的等级测评机构，每年开展一次网络安全等级测评，并及时将等级测评报告提交受理备案的公安机关和行业主管部门。新建第三级以上网络应在通过等级测评后投入运行。

整改要求。网络运营者应在网络建设和运营过程中，同步规划、建设、使用有关网络安全保护措施。应依据《网络安全等级保护基本要求》、《网络安全等级保护安全设计技术要求》等国家标准，开展网络安全建设和整改加固，全面落实安全保护技术措施。

落实安全责任。行业主管部门、网络运营者应依据法律法规和有关政策要求，建立网络安全等级保护工作责任制度，落实责任追究制度。网络运营者要定期组织专门力量开展网络安全自查和检测评估，行业主管部门要组织风险评估。

供应链安全管理及远程运维管理。网络运营者应加强网络关键人员的安全管理，第三级以上网络运营者应对为其提供设计、建设、运维、技术服务的机构和人员加强管理，评估服务过程中可能存在的安全风险，并采取相应的管控措施。网络运营者应加强网络运维管理，因业务需要确需通过互联网远程运维的，应进行评估论证，并采取相应的管控措施。

落实密码防护要求。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网

[1] https://www.mps.gov.cn/n6557558/c7369310/content.html

络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。

二、建立并实施关键信息基础设施安全保护制度

《指导意见》要求在落实网络安全等级保护制度基础上突出保护重点，明确了关键信息基础设施的认定方法、职能分工等，对关键信息基础设施保护工作的实践提供了重要指引。

关键信息基础设施认定方法。对关键信息基础设施的认定，《指导意见》提出由重点行业和领域主管、监管部门制定各行业认定规则，并报公安部备案，关键信息基础设施进行动态清单管理的认定机制：

- 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（以下统称“**保护工作部门**”）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。
- 保护工作部门认定本行业、本领域关键信息基础设施，及时将认定结果通知相关设施运营者并报公安部，包括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。
- 关键信息基础设施清单实行动态调整机制，有关网络设施、信息系统发生较大变化，可能影响其认定结果的，运营者应及时将相关情况报告保护工作部门，保护工作部门应组织重新认定，将认定结果通知运营者，并报公安部。

关键信息基础设施安全保护工作职能分工。对于关键信息基础设施工作的职能分工，《指导意见》提出：

- 公安部负责关键信息基础设施安全保护工作的顶层设计和规划部署。
- 保护工作部门负责对本行业、本领域关键信息基础设施安全保护工作的组织领导，制定并实施本行业、本领域关键信息基础设施安全总体规划和安全防护策略，落实本行业、本领域网络安全指导监督责任。
- 关键信息基础设施运营者负责设置专门安全管理机构，组织开展关键信息基础设施安全保护工作，主要负责人对本单位关键信息基础设施安全保护负总责。

此外，《指导意见》重述、强调了落实关键信息基础设施重点防护措施，加强重要数据和个人信息保护强化核心岗位人员和产品服务的安全管理等要求。

三、我们的观察

考虑到《网络安全法》等法规的笼统规定及不断变化的实践情况，《指导意见》将成为落实网络安全等级保护及关键信息基础设施相关制度的重要实践指导文件。

根据《指导意见》，网络安全等级保护制度将深入贯彻落实，无论企业所在行业及规模，根据网络安全等级保护要求进行系统定级备案、测评、整改等将成为所有企业常态化合规工作。

《网络安全法》首次提出关键信息基础设施网络安全保护要求后，法律、法规未明确关键信息基础设施制度的具体要求。《指导意见》进一步明确了关键信息基础设施的认定工作安排和监管重点。重点行业、领域的企业需进一步关注其行业或领域主管机关发布的行业认定标准及网络安全指导要求。

董　潇　合伙人　电话：86 010 8519 1718　邮箱地址：dongx@junhe.com
郭静荷　律　师　电话：86 010 8553 7947　邮箱地址：guojh@junhe.com
冯毅捷　律　师　电话：86 010 8540 8673　邮箱地址：fengyijie@junhe.com