汉坤法律评述

2021 年 8 月 18 日

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

《关键信息基础设施安全保护条例》速读

作者：段志超 | 蔡克蒙 | 汪向阳

2021 年 8 月 17 日，国务院正式公布了《关键信息基础设施安全保护条例》（**“《条例》”**），将于 2021 年 9 月 1 日起正式施行。从 2017 年征求意见至今，《条例》历时三年多终于出台。《条例》是《网络安全法》重要配套行政法规，对《网络安全法》中关于关键信息基础设施安全相关规定进行了细化和落实，将为关键信息基础设施安全保护工作提供有力法治保障。本文旨在对《条例》的要点进行梳理，解读《条例》规定的关键信息基础设施保护要求。

一、关键信息基础设施的认定机制

《条例》首先勾勒出了关键信息基础设施大致的认定机制。

- **负责认定的主体**。《条例》明确了相关重要行业、领域的主管部门和监督管理部门是关键信息基础设施的保护工作部门（**“保护工作部门”**），在公安部门统一指导下开展关键信息基础设施认定工作。
- **制定认定规则**。《条例》规定由保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则。
- **组织认定并通知结果**。《条例》规定保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，认定结果应及时通知运营者。因此，运营者的相关网络设施、信息系统是否属于关键信息基础设施系以保护工作部门认定为准，而非运营者自我判断。此外，《条例》并未要求保护工作部门公布认定结果，而仅要求将认定结果通知公安部，这可能主要是出于关键信息基础设施保护的保密性要求考虑。
- **发生变化后重新认定**。关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起 3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

二、关键信息基础设施的认定标准

《条例》第二条对关键信息基础设施基本沿用了《网络安全法》中的定义，将关键信息基础设施界定为“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，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等”。该定义从重点行业和系统信息泄露风险两个角度对关键信息基础设施进行界定，仅在《网络安全法》定义基础上增加了国防科技工业这一重要行业。

《条例》第九条第二款指出，保护工作部门制定关键信息基础设施认定规则应当主要考虑下列因素：（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；（三）对其他行业和领域的关联性影响。根据公安部 2020 年制定的《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》，可能被认定关键信息基础设施的包括“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”。

三、关键信息基础设施运营者的义务

除一般网络运营者均应履行的义务以外，下表总结了《条例》规定的关键信息基础设施运营者应履行的特别义务及对应法律责任。

序号	事项	CIIO 义务	法律责任
1	**《条例》第 11 条，CIIO 发生较大变化的报告义务。**	关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。	由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。
2	**《条例》第 12 条，安全保护措施同步规划、同步建设、同步使用。**	安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。	
3	**《条例》第 13 条，建立健全网络安全保护制度和责任制。**	运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。	
4	**《条例》第 14 条，设置专门安全管理机构，安全岗位人员背景审查。**	运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。	
5	**《条例》第 15 条，专门安全管理机构职责。**	专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责： （一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；	

序号	事项	CIIO 义务	法律责任
		（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估； （三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件； （四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议； （五）组织网络安全教育、培训； （六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度； （七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理； （八）按照规定报告网络安全事件和重要事项。	
6	**《条例》第 16 条，专门安全管理机构的经费和人员保障、参与决策权利。**	运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。	
7	**《条例》第 17 条，每年开展网络安全检测和风险评估。**	运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。	
8	**《条例》第 20 条，采购网络产品和服务签订安全保密协议。**	运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。	
9	**《条例》第 21 条，报告合并、分立、解散等情况。**	运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。	
10	**《条例》第 18 条，报告重大网络安全事件和重大网络安全威胁。**	关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。	由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责

序号	事项	CIIO 义务	法律责任
			的主管人员处 1 万元以上 10 万元以下罚款。
11	**《条例》第 19 条，采购网络产品和服务可能影响国家安全的，应进行安全审查。**	运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。	由国家网信部门等有关主管部门依据职责责令改正，处采购金额 1 倍以上 10 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 1 万元以上 10 万元以下罚款。
12	**《条例》第 28 条，配合网络安全检查检测。**	运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。	由有关主管部门责令改正；拒不改正的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节严重的，依法追究相应法律责任。

四、结语

关键信息基础设施安全保护是网络安全保护的基石，对于维护国家安全、经济健康发展、维护社会稳定和社会公共利益具有重要的意义。《条例》落实了《网络安全法》对关键信息基础设施的保护规定，在《网络安全法》的框架下，细化了关键信息基础设施运营者的义务和责任。关键信息基础设施运营应当严格按照《条例》的规定，落实主体责任，保护关键信息基础设施的安全。

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或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com

© 2021 Han Kun Law Offices. All Rights Reserved.