《关键信息基础设施安全保护条例》企业合规速览

作者：潘永建 | 朱晓阳 | 王雪莹

关键信息基础设施是数字经济时代社会运行的神经中枢，是网络安全的重中之重。保障关键信息基础设施安全，对于维护国家网络空间主权和国家安全、保障经济社会健康发展、维护公共利益和公民合法权益具有重大意义。基于此，国务院通过《关键信息基础设施安全保护条例》(“《条例》”)并于近日正式公布，旨在规范关键信息基础设施安全保护工作，维护网络安全。笔者将借本文，简要介绍关键信息基础设施(“CII”)及关键信息基础设施运营者(“CIIO”)的认定规则，并以企业视角，分析 9 月 1 日该《条例》生效后，被认定为 CIIO 的企业需要履行哪些义务，以及《条例》是否可能适用于未被认定为 CIIO 的企业。

一. 关键信息基础设施由“保护工作部门”认定

《条例》对 CII 的定义保持了此前《网络安全法》等法律的认定标准，即 CII 是指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。定义延续了过往 CII 相关法律文件所采用的“行业列举+后果概括”的复合定义方式。应当注意的是，“后果概括”为 CII 作出了兜底性的规定，因此 CII 可能不仅仅存在于定义中列举出 8 个重点行业和领域之中，其他行业和领域也可能有网络设施和信息系统被认定为 CII，且并非上述 8 个行业和领域的所有设施系统均属于 CII。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

《条例》明确规定由保护工作部门(指的是相关重要行业、领域的主管部门和监督管理部门)结合本行业、本领域实际，制定 CII 认定规则，根据认定规则负责认定本行业、本领域的 CII，并将认定结果通知相关运营者。因此，对于企业而言，无需担心因错误评估导致未能履行 CIIO 义务进而遭到处罚的风险，企业只需密切关注本行业、本领域关于 CII 认定的立法规则，与保护工作部门保持沟通交流，遵从保护工作部门的认定意见即可。

当然，这并不意味着企业的自我评估便不重要，因为企业一旦被保护工作部门认定为 CIIO，即应开始履行 CIIO 的法定义务，而从下文可以看出，这些义务的履行并不是一蹴而就，相反，是需要经过长期的布局和积累的，因此，我们建议处于上述列举行业中的企业在保护工作部门认定前，结合《条例》等法规对自身是否可能构成 CIIO 进行评估，如果自我评估后认为该等可能性较高的，则需要提前为履行 CIIO 的义务进行准备。

二. 关键信息基础设施运营者的义务

我们在第一部分中说到，CII 认定的主动权在保护工作部门，待 CII 认定完毕后，就 CII 的安全保护工作，《条例》建立了“综合协调、分工负责、依法保护”的责任结构，即:

	主体	相应的 CII 安全保护工作
自下而上	CIIO	主体责任
	省级人民政府有关部门	实施安全保护和监督管理工作
	国务院电信主管部门和其他有关部门	负责关键信息基础设施安全保护和监督管理工作
	国务院公安部门	负责指导监督关键信息基础设施安全保护工作
	国家网信部门	统筹协调

为明确 CIIO 的主体责任，《条例》进一步规定 CIIO 的主要负责人须对 CII 的安全保护负总责，这意味着，企业层面的 CII 安全保护义务须由 CIIO 的主要负责人来牵头落实。从《条例》所规定的违反 CII 安全保护义务的法律责任条款中，我们也能看出，一旦 CII 的保护措施缺位，CIIO 的主要负责人难辞其咎。

基于此思路，我们结合过往有关 CII 和 CIIO 的法律文件，总结了 CIIO 的被动义务(配合保护工作部门等有关部门的义务)和主动义务(自发采取的安全保护措施)，以及怠于履行时对 CIIO 主要负责人和企业本身带来的法律后果，供读者参考:

	被动义务	法律责任	
		直接负责的主管人员	CIIO
1.	关键信息基础设施发生较大变化可能影响其认定结果的，及时将相关情况报告保护工作部门	罚款 1 万元 - 10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 - 100 万元

2.	配合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，及时整改安全隐患、完善安全措施	罚款 1 万元 - 10 万元；情节严重的，依法追究相应法律责任	责令改正；拒不改正的，罚款 5 万 - 50 万元
3.	根据保护工作部门的要求，报送关键信息基础设施网络安全检测和风险评估相关情况	罚款 1 万元 - 10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 - 100 万元
4.	向保护工作部门、公安机关报告关键信息基础设施相关的重大网络安全事件或者重大网络安全威胁	罚款 1 万元 - 10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 - 100 万元
5.	向保护工作部门报告合并、分立、解散等情况，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	罚款 1 万元 - 10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 - 100 万元
6.	配合保护工作部门组织的网络安全事件应急演练，接受保护工作部门有关网络安全事件应对处置的指导	/	/

	主动义务	**法律责任**	
		直接负责的主管人员	**CIIO**
7.	遵守网络安全等级保护制度的要求	罚款 5000 元 - 5 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 1 万 - 10 万元
8.	制定网络安全事件应急预案，定期开展应急演练，处置网络安全事件	罚款 1 万元 - 10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 - 100 万元
9.	确保安全保护措施与关键信息基础设施同步规划、同步建设、同步使用	罚款 1 万元 - 10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 - 100 万元
10.	设置专门安全管理机构，保障其运行经费、人力资源，允许机构人员参与网络安全和信	罚款 1 万元 - 10 万元	责令改正，警告；拒不改正或者导致危害

	息化有关的决策过程		网络安全等后果的，罚款 10 万 -100 万元
11.	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，组织开展网络安全工作考核，提出奖励和惩处建议	罚款 1 万元 -10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 -100 万元
12.	对中国境内收集和产生的个人信息和重要数据本地化存储，确需出境的，开展安全评估	罚款 1 万元 -10 万元	责令改正，警告，没收违法所得，罚款 5 万 –50 万，责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照
13.	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	罚款 1 万元 -10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 -100 万元
14.	采购可能影响国家安全网络产品和服务，须按照《网络安全审查办法》通过安全审查；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；	罚款 1 万元 -10 万元	责令改正，罚款采购金额 1 倍 -10 倍
15.	对法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，使用商用密码进行保护，并自行或者委托商用密码检测机构开展商用密码应用安全性评估	罚款 1 万元 -10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 -100 万元
16.	对重要系统和数据库进行容灾备份	罚款 1 万元 -10 万元	责令改正，警告；拒不改正或者导致危害网络安全等后果的，罚款 10 万 -100 万元

附录中，我们总结了 CII 保护工作的实践操作指引，供企业在具体开展 CII 安全保护工作予以参考。

三. 非关键信息基础设施运营者的义务

《条例》是以 CIIO 的视角来起草的，但这并非意味着《条例》对于没有被认定为 CIIO 的企业没有影响。如果非 CIIO 的企业为 CIIO 提供服务，受制于《条例》第二十条和《网络安全审查办法》的规定，

需要配合 CIIO 履行网络安全审查义务，与 CIIO 签订安全保密协议，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必要的技术支持服务等。

违反相关的技术支持和安全保密义务，不仅可能导致合同责任，还可能引发行政责任，触发包括非法获取计算机信息系统数据、非法控制计算机信息系统罪在内的多项罪名的刑事风险，严重情节下，主要责任人员可能面临 7 年以下有期徒刑，并处罚金的刑事责任。

四. 结语

《条例》明确了 CII 监督及保护工作中许多亟待解决的问题，为 CII 的安全稳健运行奠定了坚实的基础。我们期待关于 CII 的认定措施和细节尽快出台，使得各行业 CII 的范围予以明确，CIIO 也可以尽快落实其法律义务。

附录

关键信息基础设施保护工作的主要法律依据和实操指引

效力层级	文件名称	
法律	《网络安全法》	该法是 CII 安全保护工作的最根本的法律依据，其中规定了一般网络运营者的安全保护义务和 CIIO 的特别义务，对于 CIIO 而言，二者义务均需严格遵守和履行。
法律	《数据安全法》	该法重申了 CIIO 对于个人信息和重要数据本地化存储的义务。
法律	《出口管制法》	该法虽然不是有关数据和 CII 的主要法律依据，但考虑到数据可能落入管制物项的范围，其可能对 CII 的安全保护工作产生一定的规制作用。
法律	《密码法》	该法规定了 CIIO 的密码保护义务。
行政法规	《关键信息基础设施安全保护条例》	该条例是《网络安全法》之后最重要的一部有关 CII 安全保护工作的法律文件。
部委规章	《网络安全审查办法》	该办法规定了 CIIO 采购网络设备和服务的安全审查义务。
内部文件	《国家网络安全检查操作指南》	该指南未正式公布，其中确定了 CII 认定的步骤，并对关键业务和 CII 进行了详细列举，我们理解在各行业和领域认定规则正式出台之前，该指南仍具有实践参考价值。
推荐性国标	《信息安全技术 关键信息基础设施网络安全保护要求》(征求意见稿)	该国标规定了对 CIIO 在识别认定、安全防护、检测评估、监测预警、应急处置等环节的基本要求，适用于 CII 的规划设计、开发建设、运行维护、退出废弃等阶段。该国标正式稿尚未发布，但我们理解待正式出台后将会成为 CIIO 开展网络安全合规工作的一项重要的指引。
推荐性国标	《信息安全技术 关键信息基础设施安全控制措施》(征求意见稿)	该国标规定了 CIIO 在风险识别、安全防护、检测评估、监测预警、应急处置等环节应实现的安全控制措施。
推荐性国标	《信息安全技术 关键信息基础设施安全防护能力评价方法》(征求意见稿)	该国标描述了 CII 安全防护能力评价模型，给出了能力评价方法，主要适用于 CIIO 对自身安全能力进行评价，也可适用于网络安全服务机构对 CIIO 安全能力进行评价。
推荐性国标	《信息安全技术 关键信息基础设施边界确定方法》(征求意见稿)	该国标提出了 CII 边界识别基本原则，给出了 CII 边界识别模型、方法和流程。

推荐性国标	《信息安全技术 关键信息基础设施安全保障指标体系》(征求意见稿)	该国标规定了用于开展 CII 安全保障的指标及其释义。
推荐性国标	《信息安全技术 关键信息基础设施安全检查评估指南》(征求意见稿)	该国标提供了 CII 检查评估工作的方法、流程和内容，定义了 CII 检查评估所采用的方法，规定了 CII 检查评估工作准备、实施、总结各环节的流程要求，以及在检查评估具体要求和内容。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野