关键信息基础设施范围有望进一步明晰

评《关键信息基础设施安全保护条例（征求意见稿）》

杨洪泉韩璐

前言

国家互联网信息办公室于 2017 年 7 月 10 日发布了《关键信息基础设施安全保护条例（征求意见稿）》（“《意见稿》”），向社会公开征求意见，本次征求意见的截止日期为 2017 年 8 月 10 日。本文分析了《意见稿》中的若干重要规定。

1. “关键信息基础设施”和“关键信息基础设施的运营者”的范围

自《中华人民共和国网络安全法》（“《网络安全法》”）提出“关键信息基础设施”及“关键信息基础设施运营者”的概念以来，其范围一直未具体明确，许多企业特别是外资企业对其自身是否落入关键信息基础设施运营者亦有诸多猜测；《网络安全法》对数据出境的若干要求亦是以是否为关键信息基础设施为界限进行监管。因此，对于关键信息基础设施及其运营者的定义及范围极为引人关注。

此次《意见稿》将关键信息基础设施的运营者定义为运行、管理重点行业领域的网络设施和信息系统的单位，同时规定了判断关键信息基础设施的标准，即此类网络设施和信息系统一旦遭到破坏、丧失功能

或者数据泄露，可能严重危害国家安全、国计民生、公共利益为损害结果，则应认定为关键信息基础设施。《意见稿》提出以下五大类单位应被认定为关键信息基础设施的运营者：

（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；

（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

（四）广播电台、电视台、通讯社等新闻单位；

（五）其他重点单位。

我们理解，上述五类行业已被划为关键信息基础设施和关键信息基础设施运营者所处的行业，但这并不意味着上述行业内的所有网络设施和信息系统都应被认定为关键信息基础设施。是否被认定为关键信息基础设施，首先须判断该网络设施和信息系统是否一经破坏或数据泄露即可能造成危害国家安全或国计民生的严重后果。例如，银行作为金融行业的典型单位，其核心业务信息系统因处理核心交易信息而极有可能被认定为关键信息基础设施，但银行内部的员工管理系统由于并不涉及危害国家安全或国计民生的风险，则不应当被认定为关键信息基础设施。

《意见稿》规定，国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南；国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。由此可见，某一行业的具体关键信息基础设施的范围取决于行业主管或监管部门对本行业、本领域的关键信息基础设施的最终认定。值得注意的是，2016 年由网信办统筹组织的全国网络安全检查中曾提出识别关键信息基础设施的三个步骤，即 1）识别可能存在关键信息基础设施的“关键业务”；2）识别潜在的关键信息基础设施（即特定信息系统）；3）使用具体标准来确定关键业务中的关键信息基础设施列表。由此可见，《意见稿》对于判定关键信息基础设施的方法论与 2016 年的“摸底”大检查所用方法论基本一致。

2. 强调对关键信息基础设施范围内的数据出境限制

本次《意见稿》规定，关键信息基础设施的“运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照个人信息和重要数据出境安全评估办法进行评估；法律、行政法规另有规定的，依照其规定。

上述规定同《网络安全法》对数据出境的限制保持一致[1]。值得注意的是，网信办此前发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》将适用于数据出境安全评估的主体由《网络安全法》下的“关键信息基础设施”运营者扩展到含义更广泛的“网络运营者”，但在后续征求意见稿中又删除了其中关于“应当在境内存储”的规定。据此，根据《网络安全法》和《意见稿》的规定，我们理解，对于数据本地化的原则性要求仍应仅适用于关键信息基础设施的运营者，而一般的“网络运营者”仅需遵守《个人信息和重要数据出境安全评估办法（征求意见稿）》规定的安全评估程序即可。目前，《个人信息和重要数据出境安全评估办法（征求意见稿）》已结束对社会意见的征集，相信该办法不久后将会正式出台，届时我们对此问题应有更清晰的判断。

《意见稿》还规定了关键信息基础设施运营者违反上述规定的法律责任。对于在境外存储网络数据，或者向境外提供网络数据的，“由国家有关主管部门依据职责责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

[1]《网络安全法》规定：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估”。

3. 明确关键信息基础设施安全保护工作的监管主体

《意见稿》规定国家行业主管或监管部门负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门在各自职责范围内负责相关网络安全保护和监督管理工作。县级以上地方人民政府有关部门按照国家有关规定开展关键信息基础设施安全保护工作。

4. 明确关键信息基础设施的运营者的合规义务

《意见稿》规定：关键信息基础设施的运营者对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本单位关键信息基础设施安全保护工作全面负责。

基本义务：《意见稿》详细规定了关键信息基础设施的运营者应履行的基本安全保护义务：“运营者应当按照网络安全等级保护制度的要

求，履行下列安全保护义务，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，严格身份认证和权限管理；

（二）采取技术措施，防范计算机病毒和网络攻击、网络侵入等危害网络安全行为；

（三）采取技术措施，监测、记录网络运行状态、网络安全事件，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密认证等措施。

其他义务：《意见稿》同时规定了关键信息基础设施的运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求，设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查；并定期对从业人员进行网络安全教育、技术培训和技能考核；对重要系统和数据库进行容灾备份，及时对系统漏洞等安全风险采取补救措施；制定网络安全事件应急预案并定期进行演练，应当组织从业人员网络安全教育培训等义务要求。并强调“运营者应当建立健全关键信息基础设施安全检测评估制度，关键信息基础设施上线运行前或者发生重大变化时应当进行安全检测评估。运营者应当自行或委托网络安全服务机构对关键信息基础设施的安全性和可能存在的风险隐患每年至少进行一次检测评估，对发现的问题及时

进行整改，并将有关情况报国家行业主管或监管部门。

网络安全管理负责人应履行的义务：《意见稿》还明确了关键信息基础设施的运营者的网络安全管理负责人应履行的职责，其中包括组织制定网络安全规章制度、操作规程并对关键岗位人员的技能考核；实施本单位网络安全教育和培训计划；组织开展网络安全检查和应急演练，应对处置网络安全事件等义务要求。同时规定关键信息基础设施的运营者网络安全关键岗位专业技术人员实行执证上岗制度。相关具体规定由国务院人力资源社会保障部门会同国家网信部门等部门另行制定。

5. 明确对运营者采购、使用的网络关键设备、网络安全专用产品的监管要求

本次《意见稿》明确了对关键信息基础设施的运营者采购网络产品和服务的相关监管要求。对可能影响国家安全的，应当按照网络产品和服务安全审查办法的要求，通过网络安全审查，并与提供者签订安全保密协议。对外包开发的系统、软件，接受捐赠的网络产品，在其上线应用前应当进行安全检测。使用的网络产品、服务存在重大安全缺陷、漏洞等风险的，应当按规定向有关部门报告。

《意见稿》同时规定，关键信息基础设施的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。

6. 明确了监测预警、应急处置和检测评估的指导方法

《意见稿》提出，由国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，并国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度。

7. 结语

关键信息基础设施这一概念自其产生之日起即引起全社会的普遍关注，《意见稿》的公布有助于澄清企业关心的一些重要问题，但其具体范围仍有赖于各行业主管部门或监管部门对其行业内关键信息基础设施的具体认定。该范围如果过大则会加重企业的合规负担，而如果该范围过小，则不利于对行业内重要信息基础设施的网络安全保护。这一范围划定工作无疑将考验各行业主管部门对其行业内网络安全保护的认知水平和监管智慧。

我们将继续关注这一领域的进展并及时进行解读。

杨洪泉律师是安杰律师事务所合伙人，他在电信、互联网和 IT、合规、劳动等领域有丰富经验，尤为擅长提供个人信息保护和网络安全领域的法律服务。