关键信息基础设施

李拓

CISP/工业互联网中级测评师/大数据分析师

界 定

关键信息基础设施

“**金融、能源、电力、通信、交通等领域的关键信息基础设施**是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。”

——习近平总书记 2016年4月19日

“按照深化标准化工作改革方案要求，整合精简强制性标准，在国家关键信息基础设施保护、涉密网络等领域制定强制性国家标准。”

——《关于加强国家网络安全标准化工作的若干意见》2016年8月12日

“建立国家关键信息基础设施目录，制定关于国家关键信息基础设施保护的指导性文件，进一步明确关键信息基础设施安全保护要求。”

——《“十三五”国家信息化规划》（国发〔2016〕73号）2016年12月15日

“建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。”

——《国家网络空间安全战略》2016年12月27日

关键信息基础设施

“保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。”

——《中华人民共和国网络安全法》2016年11月17日

“国家建立和完善网络安全标准体系，利用标准指导、规范关键信息基础设施安全保护工作。”

——《关键信息基础设施安全保护条例（征求意见稿）》2017年7月10日

关键信息基础设施定义

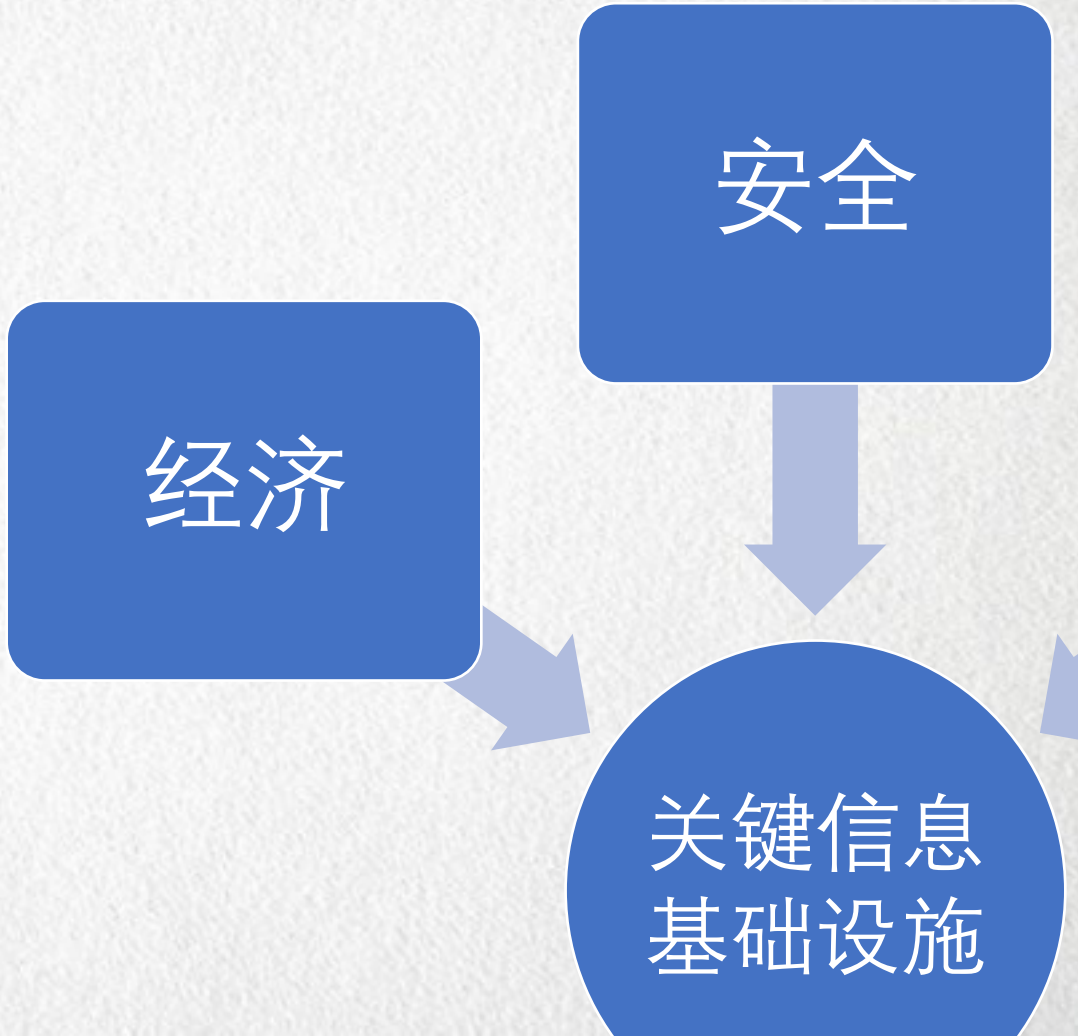
“指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施。”

——《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）》

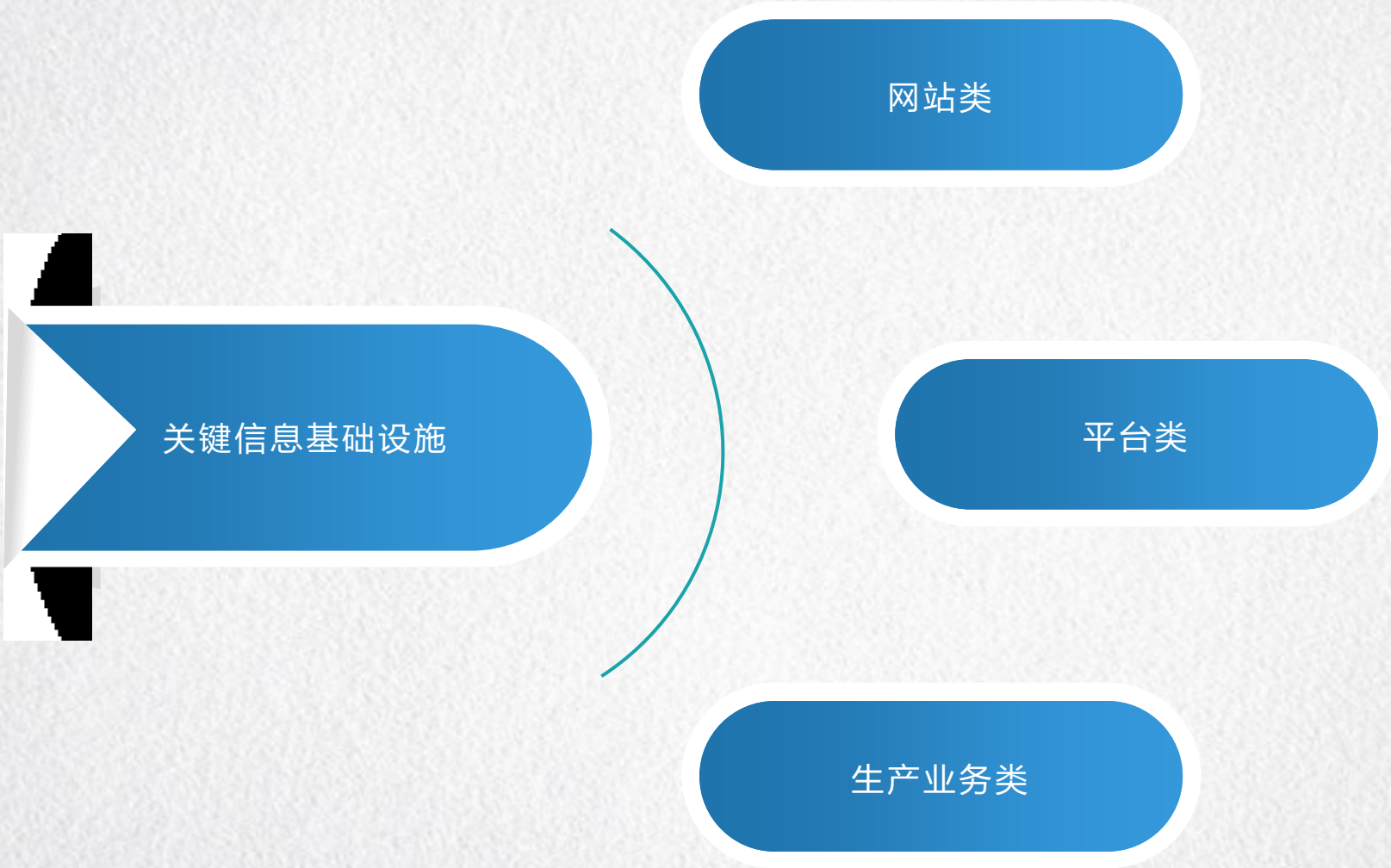
	《中华人民共和国网络安全法》	《国家网络空间安全战略》	《关键信息基础设施安全保护条例（征求意见稿）》
行业范围	公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域	包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等	（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位； （二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位； （三）国防科工、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。
危害后果	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、公共利益的关键信息基础设施	关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施	运行、管理的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、公共利益的

关键信息基础设施

- 信息和通信技术的发展使关键基础设施相互关联、相互依赖
- 实际过程中保护工作的实际对象并不是静态基础设施，而是服务、物理和电子（信息）流
- 它们为社会承担的角色和功能，尤其是通过基础设施提供的核心价值，也就是信息基础设施要素，具有重要的价值和角色，处于连接各个基础设施部门的纽带地位，支撑着其他基础设施。



关键信息基础设施分类



关键信息基础设施分类

种类	认定标准	潜在影响
网站类	1、县级（含）以上党政机关网站； 2、重点新闻网站； 3、日均访问量超过100万人次的网站； 4、一旦发生网络安全事故，可能造成右边列影响之一的； 5、其他应该认定为关键信息基础设施。	1、影响超过100万人工作、生活； 2、影响单个地市级行政区30%人口的工作、生活； 3、造成100万人个人信息泄露； 4、造成大量机构、企业敏感信息泄露； 5、造成大量地理、人口、资源等国家基础数据泄露； 6、严重损害政府形象、社会秩序，或危害国家安全。

关键信息基础设施分类

种类	认定标准	潜在影响
平台类	1、注册用户数超过1000万，或活跃数用户超过100万（每日至少登陆一次）； 2、日均成交订单额或交易额超过1000万元； 3、一旦发生网络安全事故，可能造成右边列影响之一的； 4、其他应该认定为关键信息基础设施。	1、造成1000万元以上直接经济损失； 2、直接影响超过1000万人工作、生活； 3、造成100万人个人信息泄露； 4、造成大量机构、企业敏感信息泄露； 5、造成大量地理、人口、资源等国家基础数据泄露； 6、严重损害社会和经济秩序，或危害国家安全。

关键信息基础设施分类

种类	认定标准	潜在影响
生产业务类	1、地市级以上政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关城市管理系统； 2、规模超过1500个标准机架的数据中心； 3、一旦发生网络安全事故，可能造成右边列影响之一的； 4、其他应该认定为关键信息基础设施。	1、影响单个地市级行政区30%人口的工作、生活； 2、影响10万人用水、用电、用气、用油、取暖或交通出行等； 3、导致5人以上死亡或50人以上重伤； 4、直接造成5000万以上经济损失； 5、造成100万人个人信息泄露； 6、造成大量机构、企业敏感信息泄露； 7、造成大量地理、人口、资源等国家基础数据泄露； 8、严重损害社会和经济秩序，或危害国家安全。

关键信息基础设施示例

行业	关键业务	典型信息系统及工业控制系统
广播电视	➢ 电视播出管控 ➢ 广播播出管控	电视台、广播电台的录播系统
政府部门	➢ 信息公开 ➢ 面向公众服务 ➢ 办公业务系统	地市级以上政府组成部门的办公系统、业务系统等

ansion
安 | 信 | 学 | 院

防 护 框 架

关键信息基础设施防护框架

该框架由三部分组成：**框架核心，框架轮廓和框架实现层级**。每个框架部件都会强化业务驱动因素和网络安全活动间的联系。

- 框架核心是一系列的网络安全活动、目标效果和关键基础设施部门通用的应用参考。
- 框架实现层级（Tiers）考虑网络安全风险以及使用何种流程来管理风险。
- 框架轮廓（Profile）表示组织从框架分类和子类中选择出的业务需求为基础的输出。

核心框架

- 核心提供了行业标准、指南和实践的方式，允许执行级到实施/运行级网络安全活动及效果跨组织间传递。
- 核心由五个并发的和连续的功能组成——识别、保护、检测、响应、恢复。
- 从一个组织网络安全风险管理的整个生命周期角度，提出了一个高层次，战略性的观点。
- 识别每个功能的基础主分类和子类，并使他们与实例参考文献（如每个子类的现有标准、指南和实践）相符合。

框架实现层级

◆实现层级描述了组织网络安全风险管理实践中表现出的框架中定义的特征（如，风险和威胁感知，可重复和可适应）。

◆这些实现层级表征了一定范围（从局部1级到自适应的4级）的组织实践，反映了从非正式、无响应的到敏捷的，风险警告的发展进程。

◆在实现层级选择过程中，组织应该考虑其目前的风险管理实践、威胁环境、法律和监管规定，业务目标和组织约束。

框架轮廓

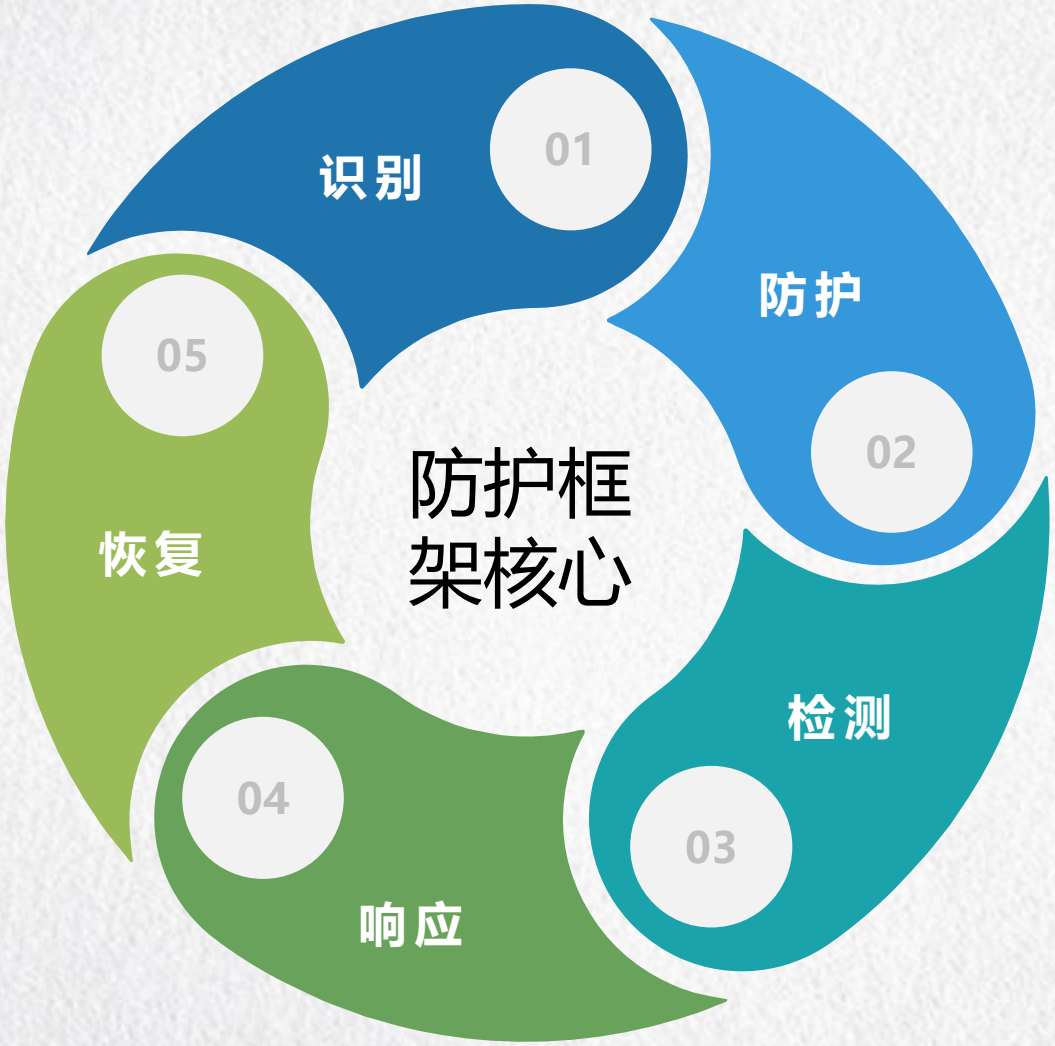
◆轮廓可以被定性为框架核心在特定实现场景下，标准、指南和实践的结合。

◆通过当前轮廓（原样状态）与目标轮廓（将来状态）相比较，确定是否改善网络安全态势。

◆为开发一个轮廓，组织可以查看所有的分类和子类，并在业务驱动因素和风险评估的基础上，确定哪些是最重要的

◆轮廓可用于进行自评估以及组织内部或者组织间的沟通。

框架核心功能



识别

帮助组织了解进而管理系统、资产、数据和能力的网络安全相关风险。

- 识别功能活动是有效使用框架的基础。理解业务内容、支持关键功能的资源以及相关的网络安全风险，使组织能够关注和优先考虑它的工作，使其与风险管理策略和业务需求保持一致。这个功能细化的例子包括：资产管理；商业环境；治理；风险评估；风险管理策略。

防护

制定和实施适当的保证措施，确保能够提供关键基础设施服务。

- 保护功能支持限制或阻止潜在网络安全事件影响的能力。此功能细化的例子包括：

  访问控制，意识和培训，数据安全，信息保护流程和规程，维护和保护技术。

检测

制定并实施适当的活动来识别网络安全事件的发生。

- 检测功能能够及时发现网络安全事件。此功能细化的例子包括：异常和事件;安全连续监测以及检测过程。

响应

制定并实施适当的活动，用以对检测的网络安全事件采取行动。

- 响应功能支持控制一个潜在的网络安全事件的影响的能力。此功能细化的例子包括：

  响应规划；通信；分析；缓解和改进。

恢复

制定并实施适当的活动，以保持计划的弹性，并恢复由于网络安全事件而受损的任何功能或服务。

- 该恢复功能支持及时恢复到正常的操作，以减轻网络安全事件的影响。此功能细化的例子包括：恢复规划；改进和通信。

整体框架流程

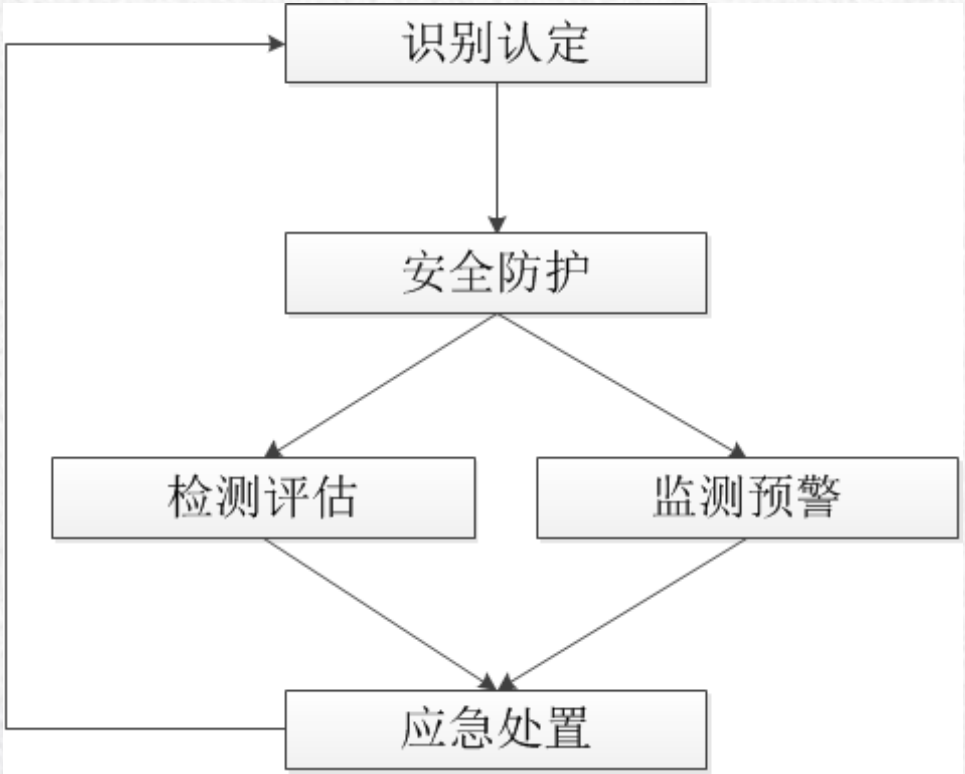
- 识别关键信息基础设施风险
- 制定并实施适当的安全防护措施
- 进行适当的行动（检测评估、安全连续监测等）判断网络安全事件是否发生
- 对检测到的网络安全事件采取行动，恢复正常运营，降低网络安全事件带来的实际影响

框架实施

- **第1步：**优先级和范围。该组织确定其业务目标和高层组织优先事项。
- **第2步：**确定方向。一旦网络安全方案的范围已根据业务线或过程确定，组织就确定了相关系统和资产，监管要求和整体风险方法。然后，组织识别这些系统和资产的威胁及其漏洞。
- **第3步：**创建一个当前轮廓。该组织通过指示需要实现的框架核心的分类和子类效果，开发一个当前轮廓。
- **第4步：**进行风险评估。
- **第5步：**创建目标轮廓。该组织创建目标轮廓，侧重于框架描述组织目标网络安全效果的分类和子类的评估。组织也根据组织的独特风险，开发自己的附加分类和子类。
- **第6步：**确定，分析和优先顺序差距。
- **第7步：**实施行动计划。

关键信息基础设施网络安全保护环节

《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）》



关键信息基础设施体系

标准名称	定位	主要内容
《信息安全技术 关键信息基础设施网络安全框架（征求意见稿）》	基础类标准	阐明了构成关键信息基础设施网络安全框架的基本要素及其关系，统一了关键信息基础设施通用术语和定义
《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）》	基线类标准	规定了对关键信息基础设施运营者在识别认定、安全防护、检测评估、监测预警、应急处置等环节的基本要求
《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）》）	实施类标准	根据基本要求规定了关键信息基础设施运营者在风险识别、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
《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）》	测评类标准	依据基本要求明确关键信息基础设施检查评估工作的方法、流程和内容，定义了关键信息基础设施检查评估所采用的方法，规定了关键信息基础设施检查评估工作准备、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
《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）》	测评类标准	规定了用于开展关键信息基础设施安全保障的指标及其释义

ansion
安 | 信 | 学 | 院

法 律 与 义 务

网络安全法明确工作重点

第三十一条 国家公共通信和信息服务、能源、交通、 水利、金融、公共服务、电子政务等重要行业和领域，以及一旦遭到破坏、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**关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护**。关键信息基础设施的具体范围和安全保护办法由国务院制定。

第四十九条 国家机关关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；**对直接负责的主管人员和其他直接负责人员依法给予处分**。

第五十九条网络运营者**不履行本法第二十一条、第二十五条**规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。关键信息基础设施的运营者不履行本法**第三十三条、第三十四条、第三十六条、第三十八条**规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
1	新建、停运需报告	**第二十条** 新建、停运关键信息基础设施，或关键信息基础设施发生重大变化的，运营者应当及时将相关情况报告国家行业主管或监管部门。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
2	确保稳定持续运行	**第二十一条** 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
3	制定安全管理制度和规程	**第二十三条第一款** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
4	防范病毒和攻击	**第二十三条第二款** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
5	留存网络日志不少于6个月	**第二十三条第三款** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
6	数据分类、备份、加密	**第二十三条第四款** 采取数据分类、重要数据备份和加密认证等措施。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
7	设立专门机构和专人	**第二十四条第一款** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
8	数据容灾备份	**第二十四条第三款** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
9	应急预案演练	**第二十四条第四款** 制定网络安全事件应急预案并定期进行演练。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
10	关键人员持证上岗	**第二十六条** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
11	从业人员每年1天以上的培训，关键人员每年3天以上的培训	**第二十七条** 运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于1个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于3个工作日。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
12	建立安全检查评估制度	**第二十八条第一款** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
13	每年不少于1次检测评估	**第二十八条第二款** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
14	限制数据跨境转移	**第二十九条** 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。	**第四十六条** 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。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
15	产品服务采购需符合国家标准	**第三十条** 运营者采购、使用的网络关键设备、网络安全专用产品，应当符合法律、行政法规的规定和相关国家标准的强制性要求。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
16	采购安全审查和签订安全保密协议	**第三十一条** 运营者采购网络产品和服务，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。	**第四十七条** 由国家有关主管部门依据职责责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
17	外包产品上线前应安全检测	**第三十二条** 运营者应当对外包开发的系统、软件，接受捐赠的网络产品，在其上线应用前进行安全检测。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
18	风险处置和报告	**第三十三条** 运营者发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向有关部门报告。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

法律与义务

序号	核心内容	具体安全保护义务	法律责任
19	境内维护	**第三十四条** 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。	**第四十五条** 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，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

ansion
安 | 信 | 学 | 院

2019

聚焦网络空间，引领未来安全