关键信息基础设施边界识别

刻不容缓

冯燕春

CII
边界识别

概念&&必要性

进展&&现状

标准主要内容

边界识别的紧迫性

CII概念

一、概念雏形

1977年，美国总统关键基础设施保护委员会（President's Council on Critical Infrastructure Protection，PCCIP）指出，美国国家安全高度依赖信息和通信、银行和金融、能源、运输等关键基础设施，这些基础设施一旦遭到攻击会给整个国家带来严重后果。据此，关键基础设施就被认为是那些一旦遭到破坏或摧毁，会对国家安全、经济发展或者公民健康造成严重影响的物质、设施、服务或者网络等。

二、概念提出

20世纪90年代起，随着信息技术发展，网络开始渗透到社会各个方面，人类拥有了通过虚拟的、非物理破坏的方式让关键基础设施停止运行的能力。1996年时任美国总统克林顿发布第13010号行政令，指出关键基础设施要么建立在脆弱的系统上，要么受到系统监视和控制，极易遭受来自网络侧的虚拟攻击。从此，在网络侧加强对关键基础设施的保护成为CIP政策新焦点，并迅速得到世界主要大国的重视。

三、概念确定

2001年美国“9·11事件”的发生，进一步提高了人们对关键基础设施脆弱性的认识。美国时任总统乔治·布什签署《爱国者法案》，将关键基础设施定义为“各种系统和资产的集合，包括虚拟和物质的。这些系统和资产对美国及其重要，其失效或者遭到破坏都会给国家安全、经济发展、公共安全造成负面影响”。此后，美国CIP政策虽多次调整，但基本上都沿用了《爱国者法案》中对关键基础设施的定义。

据统计，目前已有53个国家/地区开展了本国、本地区CI/CII保护：美国1996年，德国1997年，印度1998年，俄罗斯2000年，日本2005年，法国2006年，巴西2006年，澳大利亚2007年.....

关键基础设施领域				主管部门
1996	2002	2003	2013	
	化工和危险材料	化工	化工	国土安全部
	商业设施	商业设施	商业设施	国土安全部
电信	信息和电信	电信	通信	国土安全部
		关键制造（2008）	关键制造	国土安全部
		大坝	大坝	国土安全部
	国防工业基础	国防工业基础	国防工业基础	国防部
应急服务	应急服务	应急服务	应急服务	国土安全部
石油天然气、电力	能源	能源	能源	能源部
银行和金融	银行和金融	银行和金融	金融服务	财政部
	农业和食品	农业和食品	食品和农业	农业与卫生服务部
政府	政府	政府设施	政府设施	国土安全部
	公共健康	公共健康与保健	保健与公共健康	卫生服务部
		信息技术	信息技术	国土安全部
		核反应堆、材料和废弃物	核反应堆、材料和废弃物	国土安全部
交通运输	运输	运输系统	运输系统	国土安全部和交通部
	邮政和船运	邮政和船运		
供水系统	水	饮用水和水处理系	水及污水处理系统	环境保护局

美国关键基础设施行业变迁图

CII概念

中国：

习近平总书记4.19讲话指出，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，必须采取有效措施，切实做好国家关键信息基础设施安全防护。

《网络安全法》： 国家对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、公共利益的关键信息基础设施实施重点保护。

《关键信息基础设施安全保护条例（征求意见稿）》： 关键信息基础设施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，可能会严重危害国家安全、国计民生、公共利益的网络设施、信息系统等。

CII边界识别背景介绍

一、CII保护的目标

从国内外相关工作经验来看，国家开展CII保护的根本目标是保护重要领域内的重要业务的安全，而CII则是支撑上述关键业务安全运行的网络设施、信息系统等。

二、CII存在的基础

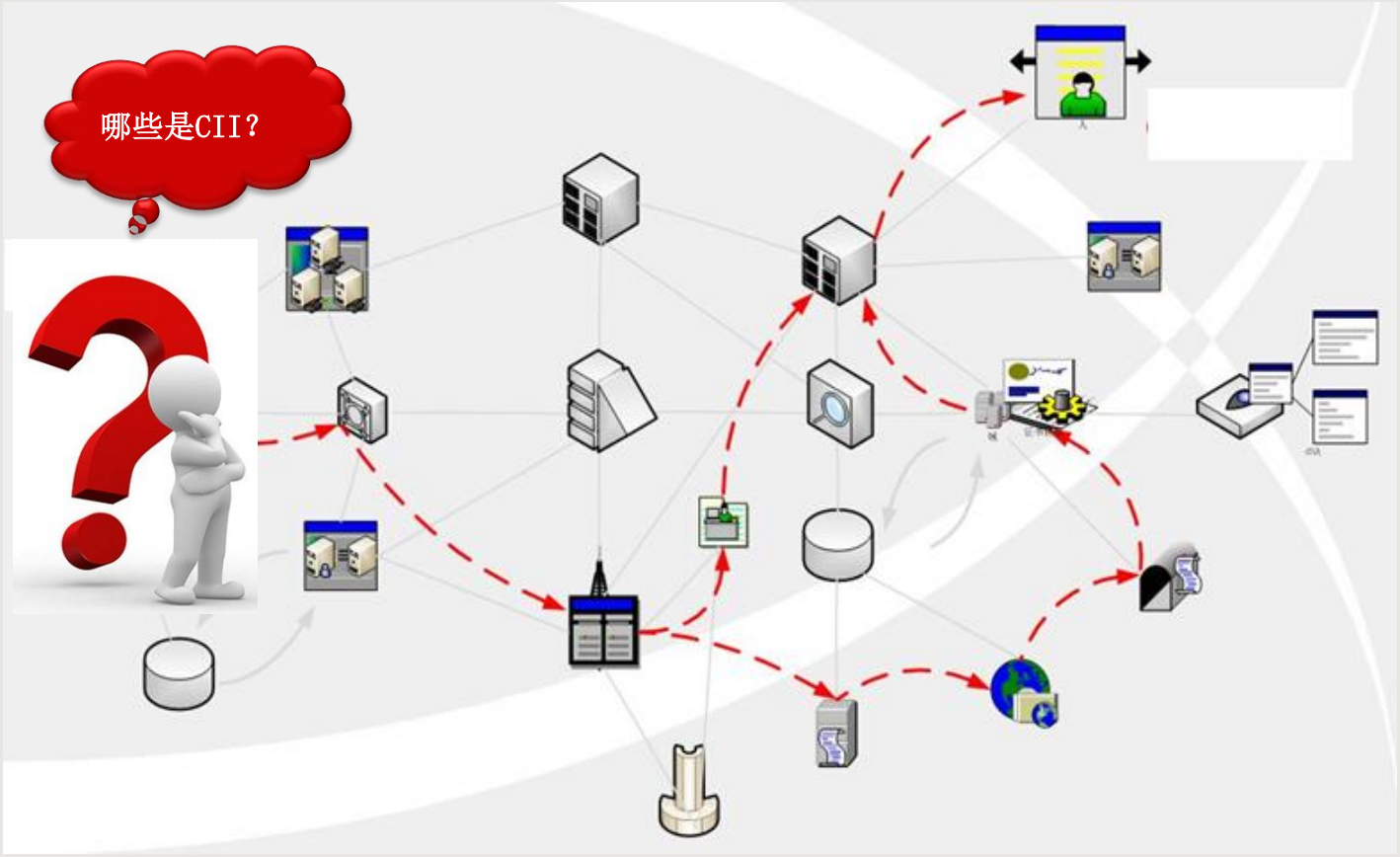
业务是CII存在的根本基础，离开业务谈CIIP是不科学的。比如大坝控制系统在形态构成、工作原理等方面都是类似的，大坝控制系统是否关键在于大坝本身的重要性。再比如，2G移动网络曾是国家主要通信设施，然而时至今日，2G网络早已被3G、4G网络所取代，虽然承载2G通信业务的网络设施、信息系统或许还在，但已经不再是国家重点保护的对象。

三、实现上述目标的关键点

CII运营者所拥有的资产设施可能会非常多，有些网络设施、信息系统对保障关键业务持续、稳定运行是非常关键（Critical）的，有些仅仅是比较重要（Important）的，甚至有一些是无关紧要（UN-important）的。因此，将关键业务持续、稳定运行所必须的网络设施、信息系统同其它信息基础设施区分开来，是CIIP护的前提和基础，对明确保护对象、实施重点保护具有重要意义。

CII边界识别概念

所谓关键信息基础设施边界，是指当运营者被国家有关部门确认为是CII运营者后，需要识别自身运营的哪些网络设施、信息系统是关键业务持续、稳定运行所必须的，应当被纳入CII保护范围。



CII边界识别示意图

CII边界识别必要性介绍

落实法律法规的基础：《中华人民共和国网安法》、《CII保护条例》等法律法规对入侵、攻击CII的不法行为做出了明确处罚措施。此外，制定中的《网络安全审查办法》、《密码法》规定运营者为CII购买设备和服务需要进行必要的安全审查、CII运营者需要按照相关规定使用密码保护，这需要明确哪些网络设施、信息系统属于CII元素。

开展保护工作的前提：将支撑关键业务持续、稳定运行的关键信息基础设施同运营者其它信息基础设施分开，明确保护对象、确定保护范围，是开展保护工作的前提和基础，对实施重点保护具有重要意义。此外，制定CII保护政策、实施CII保护规划应在CII边界已经明确的情况下进行，如果CII边界尚没有明确，开展CII保护工作显然缺乏针对性、科学性。

明确保护责任的需要：明确关键业务持续、稳定运行所必须的网络设施、信息系统，对于明确保护责任，实施一体化保护具有重要意义。

CII
边界识别

概念&&必要性

进展&&现状

标准主要内容

边界识别的紧迫性

进展&&现状--技术起源

2016年，中央网信办组建了国家关键信息基础设施网络安全检查办公室，检查办根据工作实际需要研究制定了一系列政策文件，用于指导地方、行业、企业开展关键信息基础设施检查工作，包括：《关键信息基础设施识别认定流程》、《关键信息基础设施识别认定方法》、《关键信息基础设施基线》等等。

时年，团队在国内外相关研究基础之上，结合我国关键信息基础设施保护工作实际，提出了“基于业务信息流识别关键信息基础设施边界”的技术方案。

进展&&现状--实践验证

2017年，在中央网信办指导下，云南网信办组织开展“云南省域关键信息基础设施综合试点”项目，对“基于业务信息流识别关键信息基础设施边界”进行了实践、验证、完善。

中共中央网络安全和信息化委员会办公室

Office of the Central Cyberspace Affairs Commission

WWW.CAC.GOV.CN

请输入检索关键词

首页 权威发布 办公室工作 网络安全 信息化 网络传播 国际交流 地方网信 执法督查 政策法规 互动中心 教育培训 业界动态 工作专题

当前位置：首页 > 正文

云南省委网信办部署关键信息基础设施安全保护试点示范工作

2018年07月18日 12:21:46 来源：中国网信网 【打印】 【纠错】

日前，云南省委网信办组织召开了2018年云南省关键信息基础设施安全保护试点工作部署会，贯彻习近平总书记在全国网络安全和信息化工作会议上的重要讲话精神，落实关键信息基础设施防护责任，推进全省关键信息基础设施安全保障体系建设。省委网信办副主任陈坤祥同志主持会议并讲话。

会议总结了云南省关键信息基础设施安全保护试点工作启动以来的进展，公布了入选关键信息基础设施试点示范项目的名单，并对试点工作做了安排部署。会议强调，要按照中央网信办、省委省政府的部署要求，以省域关键信息基础设施保障体系试点建设为契机和抓手，加快全省各地区各行业各领域的网络安全工作步伐，不断提升云南省网络安全保障能力和水平。

会议邀请了国家网络安全检查办成员，腾讯集团安全管理部关键信息基础设施安全保护研究专员秦小伟，就关键信息基础设施边界识别认定工作进行了专题培训。

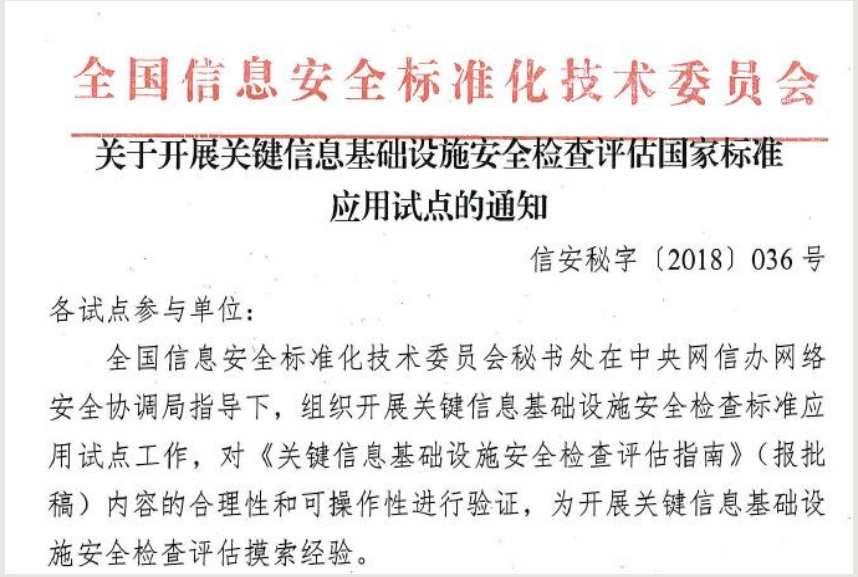
云南省级有关部门，部分重要行业领域关键信息基础设施运营单位和有关州、市委网信办负责同志共50余人参加了会议。（云南网信办供稿 作者：马兵）

进展&&现状--方案公开

2018年9月，在成都举办的国家网络安全宣传周上，团队首次公开向业内介绍了“基于信息流的关键信息基础设施边界识别认定方法”，同年在《中国信息安全》上公开发表，得到业内一定认可。

进展&&现状--方案完善、改进

2018年底，信安标委秘书处在中央网信办网络安全协调局指导下，组织开展关键信息基础设施安全检查标准应用试点工作。“基于信息流的关键信息基础设施边界识别认定方法”在此次试点中得到进一步应用和验证，同时，编制组结合此次标准试点工作对技术方案又进一步修订、改进。



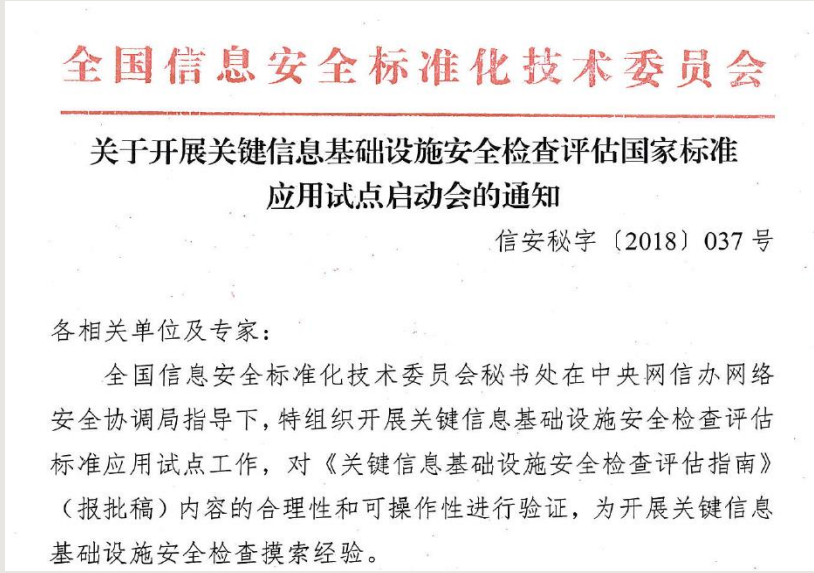
全国信息安全标准化技术委员会

关于开展关键信息基础设施安全检查评估国家标准应用试点的通知

信安秘字〔2018〕036号

各试点参与单位：

全国信息安全标准化技术委员会秘书处在中央网信办网络安全协调局指导下，组织开展关键信息基础设施安全检查标准应用试点工作，对《关键信息基础设施安全检查评估指南》（报批稿）内容的合理性和可操作性进行验证，为开展关键信息基础设施安全检查评估摸索经验。



全国信息安全标准化技术委员会

关于开展关键信息基础设施安全检查评估国家标准应用试点启动会的通知

信安秘字〔2018〕037号

各相关单位及专家：

全国信息安全标准化技术委员会秘书处在中央网信办网络安全协调局指导下，特组织开展关键信息基础设施安全检查评估标准应用试点工作，对《关键信息基础设施安全检查评估指南》（报批稿）内容的合理性和可操作性进行验证，为开展关键信息基础设施安全检查摸索经验。

进展&&现状--申请国标立项

2019年初，团队正式申请国家标准立项。2019年4月份，在宁波举办的全国信安标委会议周上被WG7推荐立项，目前在等待专家和主管部门审批正式立项。

表 1　2019 年建议立项的制定项目清单

序号	项目名称	项目类型	申报单位	备注
1.	信息技术 安全技术 公有云中作为个人可识别信息(PII)处理者的个人身份信息保护实用规则	制定	山东省标准化研究院	名称修改为《信息技术 安全技术 个人可识别信息(PII)处理者在公有云中保护 PII 的实践指南》。
2.	关键信息基础设施安全保护能力评估方法	制定	北京赛西科技发展有限责任公司	
3.	信息安全技术 电子凭据服务安全管理基本要求	制定	西安电子科技大学	《信息安全技术 电子凭据服务安全评测方法》与本标准合并，标准名称修改为《信息安全技术 电子凭据服务安全要求与测评方法》。
4.	信息安全技术 网络安全应急能力评估准则	制定	国家计算机网络与信息安全管理中心浙江分中心	
5.	信息安全技术 关键信息基础设施网络安全应急预演编制指南	制定	中国互联网络信息中心	
6.	信息安全技术 网络安全[illegible]服务要求	制定	国家计算机网[illegible]技术处理协调中心	《信息安全技术 网络安全众测服务规范》与本标准合并。
7.	信息安全技术 关键信息基础设施边界识别指南	制定	国家信息技术安全研究中心	

2

CII
边界识别

定义&&必要性

进展&&现状

标准主要内容

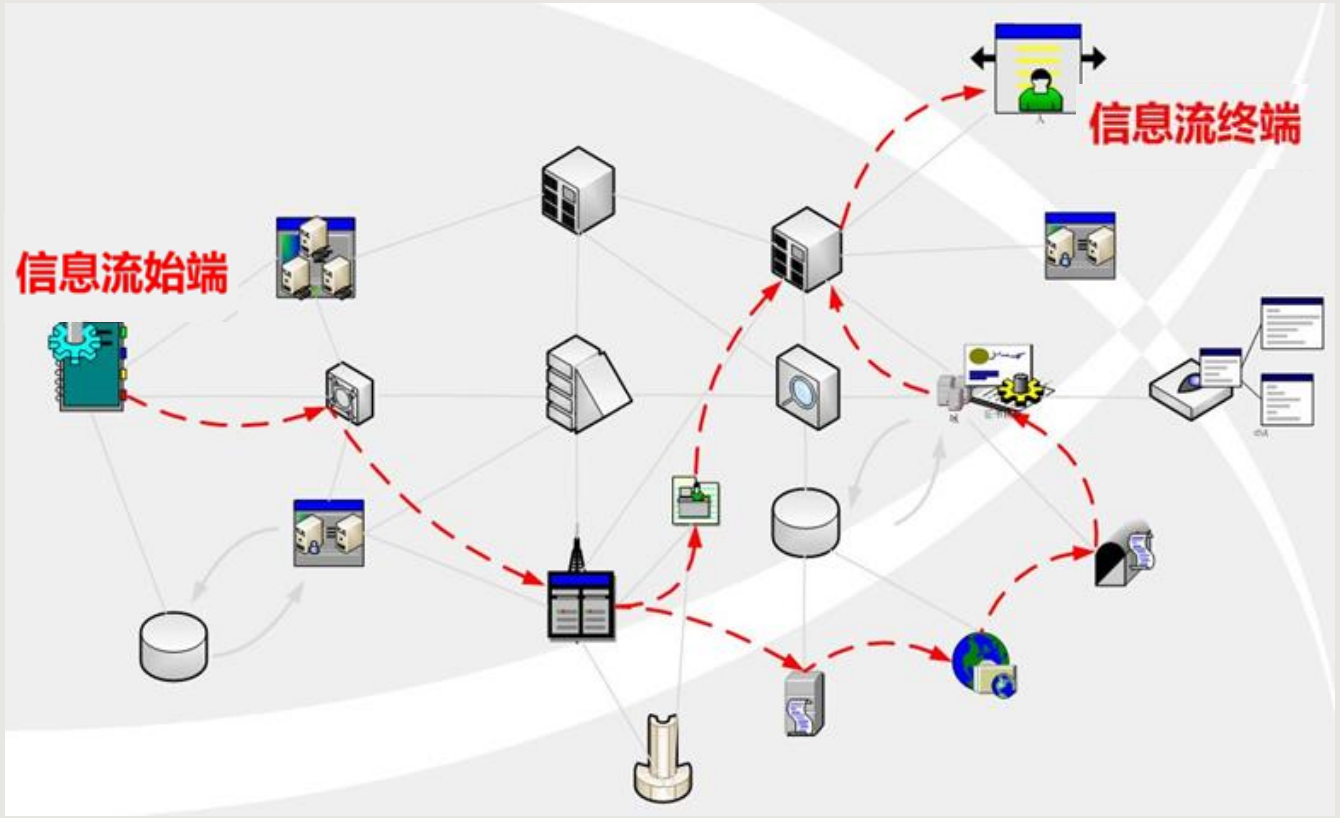
边界识别的紧迫性

标准主要内容--主要理念

一、立足点：保障CII安全的根本目的是保障关键业务的安全。

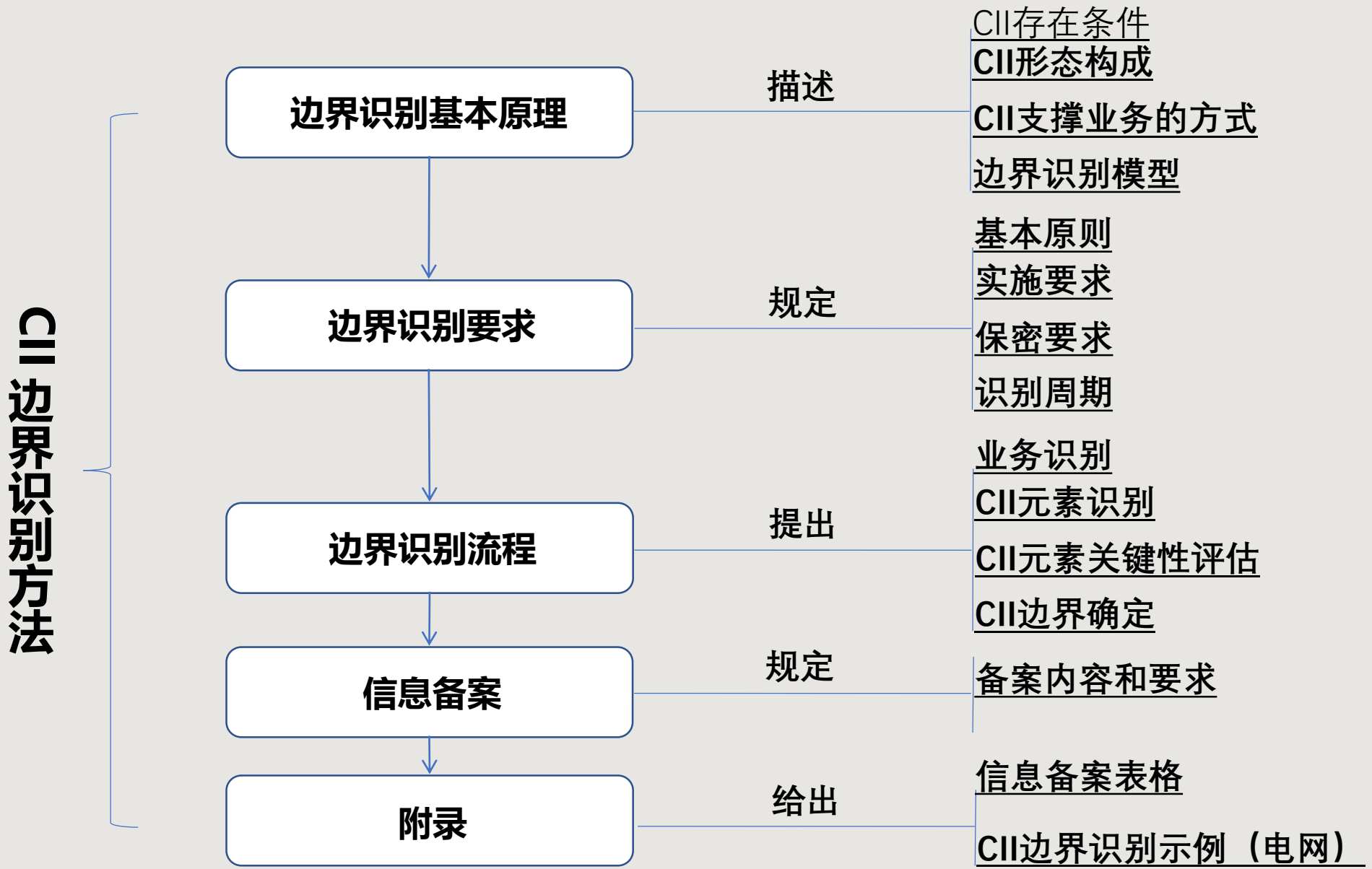
二、目标：将支撑关键业务持续、稳定运行至关重要的网络设施、信息系统同运营者其它信息基础设施区分开来，实施一体化重点保护。

三、方法：根据关键业务持续、稳定运行所必须的信息流，从产生到终止所流经的重要网络设施、信息系统组成了支撑该业务的CII。



CII边界识别示意图

标准主要内容--标准框架


CII边界识别方法
边界识别基本原理
描述
CII存在条件
CII形态构成
CII支撑业务的方式
边界识别模型
边界识别要求
规定
基本原则
实施要求
保密要求
识别周期
边界识别流程
提出
业务识别
CII元素识别
CII元素关键性评估
CII边界确定
信息备案
规定
备案内容和要求
附录
给出
信息备案表格
CII边界识别示例（电网）

CII
边界识别

概念&&必要性

进展&&现状

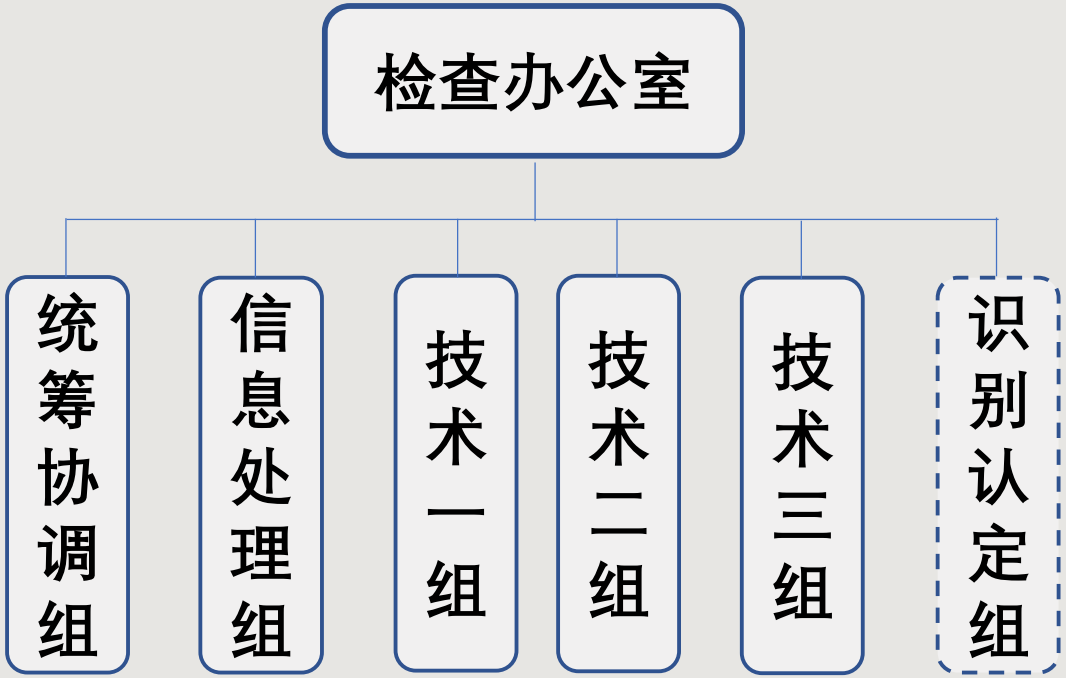
标准主要内容

边界识别的紧迫性

紧迫性介绍

国内外相关实践经验表明，在CII运营者的所有信息基础设施中，有些网络设施、信息系统对保障关键业务持续、稳定运行是非常关键的“Critical”，有些仅仅是比较重要的“Important”，甚至有一些信息设施对关键业务是无关紧要的“UN-important”。将关键的信息基础设施与其它信息基础设施区分开来，是开展关键信息基础设施保护的第一步。

保护对象不明确、保护范围不清晰，已经成为制约关键信息基础设施保护工作的瓶颈。



Disruption of information infrastructures can have a severe impact on the well-being of a nation, in terms of economic costs as well as through indirect physical damage or societal unrest. To reduce the risk of disruption of information infrastructures, a key issue is to identify which information infrastructure elements are critical to the nation and which information infrastructure elements are merely 'very important'. Separating critical elements from other elements of information infrastructures enables nations to focus protective efforts on those critical elements and to maintain national security effectively.

紧迫性介绍

《关键信息基础设施保护条例》、《网络安全审查办法》、《个人信息出境安全评估办法》等法律法规会陆续出台，这些法律法规的落实需要明确CII边界。

根据我国实际情况，根据行业、企业的重要性确定CII运营者相对容易，但当一个运营者被行业主管部门确定为是CII运营者后，如何指导运营者梳理自身运营的哪些网络设施、信息系统应纳入CII保护范畴内就是一个急需解决的问题。

国家互联网信息办公室关于《网络安全审查办法（征求意见稿）》公开征求意见的通知

中国网信网　2019-05-27 09:00:38

为提高关键信息基础设施安全可控水平，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部、国家安全部、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合起草了《网络安全审查办法（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：

国家互联网信息办公室关于《个人信息出境安全评估办法（征求意见稿）》公开征求意见的通知

国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知

2017年07月11日 09:00:02　来源：中国网信网　【打印】【纠错】

国家互联网信息办公室关于《关键信息基础设施安全保护条例（征求意见稿）》公开征求意见的通知

为保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，我办会同相关部门起草了《关键信息基础设施安全保护条例（征求意见稿）》，现向社会公开征求意见。有关单位和各界人士可以在2017年8月10日前，通过以下方式提出意见：

紧迫性介绍