ICS 35.040

L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 关键信息基础设施网络安全保护基本要求

Information security technology - Cybersecurity protection basic requirements of critical information infrastructure

在提交反馈意见时，请将您知道的相关专利连同支持文件一并附上。

（征求意见稿）

（本稿完成日期：2019-04-15）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：北京赛西科技发展有限责任公司、中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、国家工业信息安全发展研究中心、国家互联网应急中心、公安部信息安全等级保护评估中心、公安部第一研究所、中国信息安全认证中心等。

本标准主要起草人：杨建军、姚相振、王惠莅、陈亮、宋璟、孙晓丽、任卫红、周亚超、孙军、袁静等。

引　言

随着信息技术的迅猛发展，公共通信和信息服务、能源、交通、水利、金融等重要领域的系统以及服务越来越多的采用联网的方式运行或通过网络提供服务，这些重要领域的系统不仅为社会生产和居民生活提供基础公共服务，用于保证国家或地区社会经济活动正常进行的公共服务，而且承载着大量的国家基础数据、重要政务数据及公民个人信息，是网络空间安全的命脉所在，一旦遭到破坏，会对国家安全、国计民生、公共利益产生严重影响。近年来，国际上针对他国关键信息基础设施的安全攻击日趋激烈，给国家的关键信息基础设施安全甚至国家安全造成重大威胁，保护本国关键信息基础设施安全已经成国际社会关注的焦点，也成为各国维护国家网络安全的首要任务。

为落实《网络安全法》关于保护关键信息基础设施的运行安全的要求，在国家等级保护制度基础上，充分借鉴我国相关部门在重要领域网络安全审查、网络安全检查等重点工作的成熟经验，充分吸纳国外在关键基础设施安全保护方面的成功举措，结合我国现有针对传统信息系统的信息安全保障体系等成果，从识别认定、安全防护、检测评估、监测预警、事件处置等环节，提出关键信息基础设施网络安全保护要求，采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏，切实加强关键信息基础设施安全防护。

信息安全技术 关键信息基础设施网络安全保护基本要求

1 范围

本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、事件处置等环节的基本要求。

本标准适用于关键信息基础设施运营者开展关键信息基础设施安全保护工作，可用于关键信息基础设施的规划设计、开发建设、运行维护、退出废弃等阶段，也可供关键信息基础设施安全保护工作部门和关键信息基础设施安全保护的其他参与者参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 25069 信息安全技术 术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

3 术语和定义

GB/T 25069、GB/T 20984、GB/T 29246-2017 中界定的以及下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure

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、公共利益的信息设施。

4 关键信息基础设施网络安全保护基本要求

4.1 概述

本标准所指的关键信息基础设施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、工业控制系统等，其一旦遭到破坏、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。

本标准所指的关键信息基础设施运营者（以下简称运营者）负责关键信息基础设施的运行、管理，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。

本标准所指的关键信息基础设施安全保护工作部门（以下简称保护工作部门），即所属行业或领域的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运行安全保护工作。

关键信息基础设施网络安全保护包括识别认定、安全防护、检测评估、监测预警、事件处置五个环节，在GB/T22239网络安全等级保护所定等级的基本要求上展开，如图1所示。

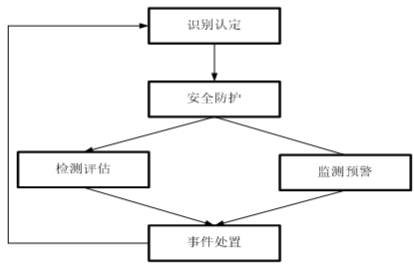

图1 关键信息基础设施网络安全保护各环节关系图

a）识别认定：运营者配合保护工作部门，按照相关规定开展关键信息基础设施识别和认定活动，围绕关键信息基础设施承载的关键业务，开展业务依赖性识别、风险识别等活动。本环节是开展安全防护、检测评估、监测预警、事件处置等环节工作的基础。

b）安全防护：运营者根据已识别的安全风险，实施安全管理制度、安全管理机构、安全管理人员、安全通信网络、安全计算环境、安全建设管理、安全运维管理等方面的安全控制措施，确保关键信息基础设施的运行安全。本环节在认定关键信息基础设施及识别其安全风险的基础上制定安全防护措施。

c）检测评估：为检验安全防护措施的有效性，发现网络安全风险隐患，运营者制定相应的检测评估制度，确定检测评估的流程及内容等要素，并分析潜在安全风险可能引起的安全事件。

d）监测预警：运营者制定并实施网络安全监测预警和信息通报制度，针对即将发生或正在发生的网络安全事件或威胁，提前或及时发出安全警示。

e）事件处置：对网络安全事件进行处置，并根据检测评估、监测预警环节发现的问题，运营者制定并实施适当的应对措施，恢复由于网络安全事件而受损的功能或服务。

4.2 识别认定

4.2.1 业务识别

运营者应：

a）识别本组织的关键业务和关键业务所依赖的外部关键业务。

b）当关键业务为外部关键业务提供服务时，识别本组织关键业务对外部关键业务的重要性。

c）梳理关键业务链，明确支撑本组织关键业务的关键信息基础设施分布和运营情况。

d）梳理关键业务链及其所需的信息流，识别关键信息基础设施的最大可能边界。

4.2.2 资产识别

运营者应：

a）识别关键业务链所依赖的资产，建立关键业务链相关的网络、系统、服务和其他资产清单。

b）基于资产类别、资产重要性和支撑业务的重要性，对资产进行优先排序，确定资产防护的优先级。

c）实现对关键信息基础设施相关资产的自动化管理，根据关键业务链所依赖资产的实际情况实时动态更新。

4.2.3 风险分析

运营者应根据关键业务链开展安全风险分析，识别关键业务链各环节的主要安全风险点，确定风险处置的优先级。

4.2.4 重大变更

运营者应当关键信息基础设施发生改建、扩建等重大变化有可能影响认定结果时，例如网络拓扑、业务链改变等，重新开展识别工作，并更新资产清单，及时将相关情况报告保护工作部门，按规定进行重新认定。

4.3 安全防护

4.3.1 安全管理制度

运营者应：

a）建立适合本单位的网络安全保护计划，结合关键业务流的安全风险分析，明确关键信息基础设施网络安全保护工作的目标、安全策略、组织架构、管理制度、技术措施、实施细则及资源保障等，形成文档并经审批后发布至相关人员。网络安全保护计划应至少每年修订一次，或发生重大变化时进行修订。

b）基于关键业务链、供应链等安全需求建立或完善安全管理制度。

4.3.2 安全管理机构

运营者应建立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主要负责人担任，设置专门的网络安全管理机构，建立并实施网络安全考核及监督问责机制。

4.3.3 安全管理人员

运营者应：

a）对安全管理机构的负责人和关键岗位的人员进行安全背景审查，符合要求的人员方能上岗，关键岗位包括与关键业务系统直接相关的系统管理、网络管理、安全管理等岗位。关键岗位应专人负责，并配备 2 人以上共同管理。

b）运营者应建立网络安全教育培训制度，定期开展基于岗位的网络安全教育培训和技能考核，教育培训内容应包括网络安全相关制度和规定、网络安全保护技术、网络安全风险意识等，关键信息基础设施从业人员的年度培训时长不少于 8 个学时，网络安全关键岗位从业人员的年度培训时长不少于 24 个学时。

c）在上岗前对人员进行安全背景审查，当必要时或人员的身份、安全背景等发生变化时应根据情况重新进行安全背景审查。应在人员发生内部岗位调动时，重新评估调动人员对关键信息基础设施的逻辑和物理访问权限，修改访问权限并通知相关人员或角色。应在人员离岗时，及时终止离岗人员的所有访问权限，收回与身份认证相关的软硬件设备，进行离职面谈并通知相关人员或角色。

4.3.4 安全通信网络

4.3.4.1 互联安全

运营者应：

a） 建立或完善不同等级系统、不同业务系统、不同区域之间的安全互联策略。

b） 保持不同等级系统、不同业务系统、不同区域之间的用户身份（例如统一身份与授权管理系统/平台）、安全标记、访问控制策略等的一致性。

c） 加强不同局域网之间远程通信时的安全防护，在通信前基于密码技术对通信的双方进行验证或认证。

4.3.4.2 边界防护

运营者应：

a） 对不同等级系统、不同业务系统、不同区域之间的互操作、数据交换和信息流向进行严格控制。

b） 加强对未授权设备的动态检测及管控能力，只允许通过运营者自身授权和安全评估的软硬件运行。

4.4.3.3 安全审计

运营者应加强网络审计措施，监测、记录系统运行状态、日常操作、故障维护、远程运维等，留存相关日志数据不少于12个月。

4.3.5 安全计算环境

4.3.5.1 鉴别与授权

运营者应：

a） 加强对设备、用户、服务或应用、数据的安全管控，对于重要业务操作或异常用户操作行为，建立动态的或额外的身份鉴别。

b） 针对重要业务数据资源的操作，基于安全标记等技术实现访问控制。

4.3.5.2 入侵防范

运营者应：

a） 实现或完善对新型网络攻击行为（如APT攻击）的入侵防范。

b） 增强系统的主动防护能力，及时识别并阻断入侵和病毒行为。

4.3.5.3 数据安全防护

运营者应：

a） 将在我国境内运营中收集和产生的个人信息和重要数据存储在境内，因业务需要，确需向境外提供数据的，应当按照国家相关规定和标准进行安全评估，法律、行政法规另有规定的，依照其规定。

b） 加强数据的全生命周期安全管理，基于数据分类分级实现相应的数据安全保护。

c） 严格控制重要数据的公开、分析、交换、共享和导出等关键环节，并采取加密、脱敏、去标识化等技术手段保护敏感数据安全。

d） 加强或完善业务连续性管理及容灾备份机制，重要系统和数据库实现异地备份。

e） 业务数据安全性要求高的实现数据的异地实时备份。

f） 业务连续性要求高的实现业务的异地实时切换，确保关键信息基础设施一旦被破坏，可及时进行恢复和补救。

4.3.5.4 自动化管理

运营者应使用自动化机制来支持系统账户、配置、漏洞、补丁、病毒库等的管理。

4.3.6 安全建设管理

运营者应：

a）在新建或改建、扩建关键信息基础实施设施，充分考虑网络安全因素，在规划、建设和投入使用阶段保证安全措施的有效性，加强设计评审、实施监理、验收评审等管控措施。必要时，可建设关键业务的仿真环境。

b）从供应商选择、安全责任划分、供应链信息保护等方面采取保护措施，避免或降低供应链安全风险。

c）采购、使用的网络产品和服务，应符合法律、行政法规的规定和相关国家标准的要求。

d）采购、使用的网络产品和服务，应通过国家规定的检测认证，可能影响国家安全的，应当通过国家安全审查。

e）发现使用的网络产品、服务存在安全缺陷、漏洞等风险时，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保护工作部门报告。

f）采购网络产品和服务时，应明确提供者的安全责任和义务，要求提供者做出必要安全承诺，并参考附录 A 签订安全保密协议。

4.3.7 安全运维管理

运营者应：

a）保证关键信息基础设施的运维地点位于中国境内，如确需境外运维，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，并事先报国家行业主管或监管部门和国务院公安部门。

b）确保优先使用现有运维工具，如确需使用由维护人员带入关键信息基础设施内部的维护工具，应在使用前通过恶意代码检测等测试。

4.4 检测评估

4.4.1 检测评估制度

运营者应建立健全关键信息基础设施安全检测评估制度，应包括但不限于检测评估流程、合规检查、技术检查、分析评估等。

4.4.2 检测评估方式和内容

运营者应：

a）自行或者委托网络安全服务机构对关键信息基础设施安全性和可能存在的风险每年至少进行一次检测评估，并及时整改发现的问题。

b）检测评估内容包括但不限于网络安全制度落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、技术防护情况、风险评估情况、应急演练情况、网络安全等级保护工作落实情况等，尤其关注关键信息基础设施跨系统、跨区域间的信息流动，及其关键业务流动过程中所经资产的安全防护情况。

c）将检测评估结果和整改情况及时上报保护工作部门。

d）新建关键信息基础设施，或关键信息基础设施在改建、扩建中发生重大变化时，应自行或者委托网络安全服务机构进行检测评估，评估变更部分所引起的业务信息流的变更，评估是否引入新的风险，并对发现的安全问题进行有效整改后方可上线。

4.4.3 抽查检测

运营者应积极配合相关部门开展的关键信息基础设施的安全风险抽查检测工作，提供网络安全管理制度、网络拓扑图、重要资产清单、关键业务介绍、网络日志等必要的资料和技术支持，针对抽查检测工作中发现的安全问题和风险进行及时整改。

4.5 监测预警

4.5.1 监测预警制度

运营者应：

a）按照保护工作部门网络安全监测预警和信息通报的要求，制定自身的监测预警和信息通报制度，确定网络安全预警分级标准，明确监测策略、监测内容和预警流程，对关键信息基础设施的网络安全风险进行监测预警。

b）建立关键信息基础设施的预警信息响应处置程序，明确不同级别预警的报告、响应和处置流程。

c）建立通报预警及协作处置机制，建立和维护外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

d）加强组织机构内部管理人员、内部网络安全管理机构与内部其他部门之间的沟通与合作，定期召开协调会议，共同研判、处置网络安全问题。

e）加强与保护工作部门、研究机构、网络安全服务机构、业界专家之间的沟通与合作，建立网络安全信息共享渠道，共享的信息可以是漏洞信息、威胁信息、最佳实践、前沿技术等。

4.5.2 监测

运营者应：

a）加强对关键业务所涉及的信息系统进行监测（例如：对加密通信进行监测，对应用层进行监测，对不同等级系统、不同业务系统、不同区域之间的信息流动进行监测等），对监测获得的信息采取保护措施，防止其受到未授权的访问、修改和删除。

b）分析信息系统通信流量或事态的模式，制定常见系统通信流量或事态的模型，并使用这些模型调整监测设备，以减少误报和漏报。

c）采用自动化机制对关键业务所涉及的信息系统的所有监测信息进行整合分析，以便及时关联、分析关键信息基础设施的网络安全态势。

d）能对将关键业务运行所涉及的各类信息进行关联，并分析整体安全态势。包括：分析不同存储库的审计日志并使之关联；系统内多个组件的审计记录进行关联；将取自审计记录的信息与得自物理访问监控的信息关联；将来自非技术源的信息（例如供应链活动信息、关键岗位人员信息等）与审计信息关联；网络安全信息共享信息关联等。

e）通过安全态势分析结果来确定安全策略和安全控制措施是否合理有效，必要时进行更新。

4.5.4 预警

运营者应

a）在发现可能危害关键业务的迹象时，监测机制应能采用自动化的方式及时报警，并自动化地采取对关键业务破坏性最小的行动。例如：恶意代码防御机制、入侵检测设备或者防火墙等弹出对话框、发出声音或者向相关人员发出电子邮件等方式进行报警。

b）对网络安全共享信息和报警信息等进行综合分析、研判，必要时生成内部预警信息。对于可能造成较大影响的，应按照保护工作部门网络安全信息通报的要求进行通报。内部预警信息的内容应包括：基本情况描述、可能产生的危害及程度、可能影响的用户及范围、建议采取的应对措施等。

c）当内部预警信息发出之后，情况出现新的变化，运营者应向有关人员和组织及时补发最新内部预警信息。

d）能持续获取预警发布机构的安全预警信息，分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度，必要时启动应急预案。并按照规定通报给相关人员和相关部门。

f）通过采取相关措施对预警进行响应，当安全隐患得以控制或消除时，应执行预警解除流程。

4.6 事件处置

4.6.1 事件管理制度

运营者应：

a）具备网络安全事件的处理能力，建立网络安全事件管理制度，明确不同网络安全事件的分类分级、不同类别和级别事件处置的流程等，制定应急预案等网络安全事件管理文档。

b）为网络安全事件处置提供相应资源，指定专门网络安全应急支撑队伍、专家队伍，保障安全事件得到及时有效处置。

c）按照相关规定参与和配合国家网信部门、保护工作部门开展的网络安全应急演练、应急处置等工作。

4.6.2 应急预案

运营者应：

a) 在国家网络安全事件应急预案的框架下，根据行业和地方的特殊要求，制定本组织的网络安全事件应急预案。应急预案中应明确，一旦信息系统中断、受到损害或者发生故障时，需要维护的关键业务功能，并明确遭受破坏时恢复关键业务和恢复全部业务的时间。应急预案不仅应包括本组织应急事件的处理，也应包括多个组织间的应急事件的处理（若适用）。

b) 在制定应急预案时，同所涉及到的运营者内部相关计划（例如业务持续性计划、灾难备份计划等）以及外部服务提供者的应急计划进行协调，以确保连续性要求得以满足。

c) 对网络安全应急预案定期进行评估修订，并持续改进。

d) 每年至少组织 1 次跨组织、跨地域的应急演练。

4.6.3 响应和处置

4.6.3.1 事件报告

运营者应：

a）当发生有可能危害关键业务的安全事件时，应及时向安全管理机构报告，并组织研判，形成事件报告单。

b）及时将可能危害关键业务的安全事件通报到可能受影响的内部部门和人员，并按照规定向关键业务供应链涉及的、与事件相关的其他组织通报安全事件。

4.6.3.2 事件处置

运营者应：

a）按照事件处置流程、应急预案进行事件处置，恢复关键业务和信息系统到已知的状态。

b）在事件发生后尽快收集证据，按要求进行信息安全取证分析，并确保所有涉及的响应活动被适当记录，便于日后分析。

c）在事件处理完成后，应采用手工或者自动化机制形成完整的事件处理报告。事件处理报告包括：不同部门对事件的处理记录、事件的状态和取证相关的其他必要信息、评估事件细节、趋势和处理。

d）在恢复关键业务和信息系统后，应对关键业务和信息系统恢复情况进行评估，查找事件原因，并采取措施防止关键业务和信息系统遭受再次破坏、危害或故障。

e）在进行事件处理活动时，协调组织内部多个部门和外部相关组织，以更好的对事件进行处理，并将事件处理活动的经验教训纳入事件响应规程、培训以及测试，并进行相应变更。

4.6.3.3 事件通报

运营者应及时将安全事件及其处置情况通报到可能受影响的部门和相关人员，向关键业务供应链涉及的、与事件相关的其他组织提供安全事件信息，并按照相关规定通报主管部门。

4.6.4 重新评估

运营者应根据检测评估、监测预警中发现的安全隐患和发生的安全事件，以及处置结果开展综合评估，必要时重新开展风险识别，并更新安全策略。

附 录 A
（资料性附录）
安全保密协议模版

甲方单位名称：_____ 地址：_____

乙方单位名称：_____ 地址：_____

本协议于_____年_____月_____日起生效

根据我国有关网络安全及信息保密相关法律法规，本着平等、自愿、公平、诚信的原则，双方就采购网络产品和服务事宜及后续合作过程中有关网络安全保密事项达成以下协议，并由双方共同遵守。采购网络产品和服务的一方应为“甲方”，提供网络产品和服务的一方应为“乙方”。

A.1 保密内容和范围

甲乙双方确认，承担保密义务的对方信息包括但不限于以下内容：

(1) 技术信息：_____（例如：同对方业务相关的程序、代码、流程、方法、文档、数据等内容）；
(2) 业务信息：_____（例如：同对方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息）；
(3) 安全信息：_____（例如：包括账号、口令、密钥、授权等用于对网络、系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息）。
(4) 其他约定的信息_____。

A.2 保密义务

A.2.1 双方明确所接收的保密信息及其载体均为对方所有。双方承认对方在本协议规定的保密信息上的利益和或一切有关的权利，双方应当考虑对方的利益并对该信息予以妥善保管。

A.2.2 双方遵守相关法律、法规、政策、规章、制度和协议，基于授权的基础上，合理使用对方信息，不得以任何其他手段获取、授权或协议规定以外的对方信息。

A.2.3 未经授权，不应在工作职责授权范围以外使用、分享对方信息。未经授权，不得泄露、披露、转让以下信息：

(1) 技术信息：_____（例如：同对方业务相关的程序、代码、流程、方法、文档、数据等内容）；
(2) 业务信息：_____（例如：同对方业务相关的人员、财务、策略、计划、资源消耗数量、通信流量大小等业务信息）；
(3) 安全信息：_____（例如：包括账号、口令、密钥、授权等用于对网络、系统、进程等进行访问的身份与权限数据，还包括对正当履行自身工作职责所需要的重要、适当和必要的信息）。

(4) 其他约定的信息_____。

A.2.4 如需向第三方披露对方信息时，应经得对方授权，因履行我国法律要求而需要披露时除外。

A.2.5 乙方对违反协议或可能导致违反协议、规定、规程、法律的活动、策略或实践，一经发现，应立即通告甲方。

A.2.6 合同结束后，应返还对方本协议中规定的信息和对方数据，包括原件和所有据此制作的副本。

A.3 违约责任

双方承认并明确同意：其对本协议的任何违约仅有法律的救济尚且不足，并且因其违约行为而造成的对方损失是难以用金钱来衡量的。因此，当一方出现任何违约情形时，另一方有权要求对方立即返还相关保密信息，且对方有义务立即采取合理补救措施。同时，对方还应赔偿：

(1) 因一方违约行为，而使另一方遭受的全部经济损失（包括直接损失和间接损失）；

(2) 一方因调查另一方的违约行为、采取补救措施而支出的所有合理费用（包括但不限于一方向另一方及第三方追索、取证、调研而发生的仲裁费、诉讼费、律师费、交通费、劳务费等）。

A.4 协议有效期

本协议自生效日起___年内一直保有完全的效力。本协议有效期内任何时间双方可通过相互同意或向另一方发出书面通知天后终止协议；但提前终止本协议不应豁免双方在本协议下就终止生效日前提供给对方保密信息所应履行的义务。

A.5 如果所涉及的保密信息依照国家主管机关或相关法律、法规另有规定的，适用其相关规定。

甲方签字（盖章） 乙方签字（盖章）

年 月 日 年 月 日

参考文献

[1]《中华人民共和国网络安全法》，2016
[2]《关键信息基础设施安全保护条例（征求意见稿）》，2017
[3]《个人信息和重要数据出境安全评估办法（征求意见稿）》，2017
[4] GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南
[5] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
[6] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南
[7] GB/T 32921-2016 信息安全技术 信息技术产品供应方行为安全准则
[8] GB/T 32924-2016 信息安全技术 网络安全预警指南
[9] Framework for Improving Critical Infrastructure Cybersecurity
[10] NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations