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 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：2018-03-18）

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、中国信息安全认证中心、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等。

本标准主要起草人：

引　言

随着信息技术的迅猛发展，金融、能源、交通等重要领域的系统、设备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，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、经济稳定和公众安全产生严重影响。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，在等级保护基础上，从识别认定、安全防护、检测评估、监测预警、应急处置等环节，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。

《关键信息基础设施网络安全框架》作为基础标准，阐明构成框架的基本要素及其关系，统一通用术语和定义；本标准作为基线类标准，对关键信息基础设施运营者开展网络安全保护工作提出最低要求；《关键信息基础设施安全控制措施》作为实施类标准，根据基本要求提出相应的控制措施；《关键信息基础设施安全检查评估指南》作为测评类标准，依据基本要求明确关键信息基础设施检查评估的目的、流程、内容和结果；《关键信息基础设施安全保障指标体系》作为测评类标准，依据检查评估结果、日常安全检测等情况对关键信息基础设施安全保障状况进行定量评价。

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、应急处置等环节的基本要求。

本标准适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。

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 25069-2010 信息安全技术 术语

GB/T 29246-2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T XXXXX-XXXX 信息安全技术 网络产品和服务通用安全要求

3 术语和定义

GB/T 25069-2010、GB/T 20984-2007 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。

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（以下简称安全保护工作部门），即所属行业或领域的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、应急处置五个环节，在网络安全等级保护原定等级的基本要求上展开，如图1所示。

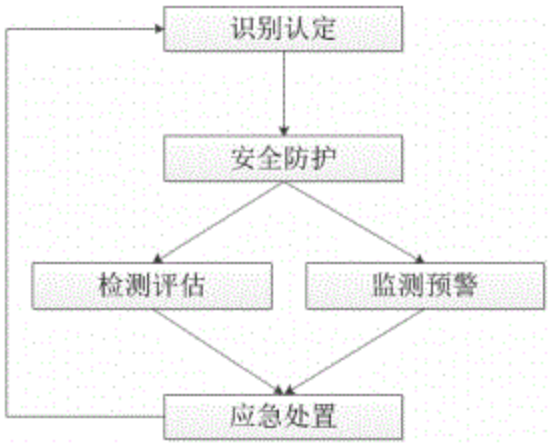

图 1 关键信息基础设施网络安全保护各环节关系图

——识别认定：运营者配合安全保护工作部门，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，开展风险识别。本环节是开展安全防护、检测评估、监测预警、应急处置等环节工作的基础。

——安全防护：运营者根据已识别的安全风险，在规划、人员、数据、供应链等方面制定和实施适当的安全防护措施，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。

——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。

——监测预警：为检验安全防护措施的有效性，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。

——应急处置：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，并恢复由于网络安全事件而受损的功能或服务，动态识别关键信息基础设施的安全风险。

4.2 识别认定

4.2.1 运营者应梳理关键业务链，建立关键业务链相关的网络、系统和资产清单。

4.2.2 运营者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，明确安全防护优先级。

4.2.3 新建、停运关键信息基础设施，或关键信息基础设施发生改建、扩建等重大变化时，运营者应当重新开展自识别工作，并更新网络、系统和资产清单，及时将相关情况报告安全保护工作部门。

4.3 安全防护

4.3.1 运营者应围绕安全组织与人员、数据安全、系统和通信保护、审计、维护、系统开发与供应链安全、访问控制、配置管理、物理与环境安全等方面开展安全防护活动，应制定相应安全策略和操作规程，定期更新，并采取相应的安全技术措施。

4.3.2 运营者应设置专门的网络安全管理机构，负责健全完善网络安全管理制度，落实网络安全防护措施，组织实施监督检查和教育培训等工作。

4.3.3 运营者应制定关键信息基础设施安全责任制度，明确相关安全责任人，包括内部人员、外部人员的安全角色和安全职责。

4.3.4 安全管理机构的负责人应由运营者主要负责人担任，并对该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。

4.3.5 运营者应建立适合本单位的网络安全计划，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、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。网络安全计划应至少每年修订一次。

4.3.6 运营者新建或改建、扩建关键信息基础设施时，应充分考虑网络安全因素，实现安全技术措施同步规划、同步建设、同步使用。

4.3.7 运营者应建立网络安全教育培训制度，定期开展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，原则上关键信息基础设施从业人员的年度培训时长不少于1个工作日，网络安全关键岗位从业人员的年度培训时长不少于3个工作日。

4.3.8 运营者应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，并采取数据分类分级、重要数据备份和加密认证等技术措施和其他必要措施，防止信息泄露、毁损、丢失，确保其收集的信息安全。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》进行安全评估；法律、行政法规另有规定的，依照其规定。

4.3.9 运营者应根据承载业务的重要性和数据的敏感程度，对关键信息基础设施实施分区分域管理，制定关键信息基础设施不同区域的访问控制策略，部署边界防护措施，避免重要网络、系统和资产遭受未经授权的访问，防止重要数据泄露或者被窃取、篡改。

4.3.10 运营者应只允许经过运营者自身授权和安全评估的软硬件运行，并应建立计算机病毒和网络入侵防范机制，严格限制未授权的临时设备接入。

4.3.11 运营者应采取审计措施，监测、记录系统运行、操作、故障维护等行为，并留存相关日志，尤其要对远程运维的行为进行严格的控制和审计。相关的系统、网络设备日志留存不少于6个月。日志内容应至少包括：事件的日期和时间、类型、主体、客体、结果等信息。

4.3.12 运营者应对重要系统和数据库进行容灾备份，制定容灾备份策略，规定备份频率，并定期执行，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。

4.3.13 运营者采购、使用的网络产品和服务应当符合GB XXXXX-XXXX《信息安全技术 网络产品和服务通用安全要求》标准要求，并应在其上线应用前进行安全检测。当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安全保护工作部门报告。

4.3.14 运营者采购网络产品和服务时，应在与提供者的合同中，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，并对提供者履约情况进行核实。

4.3.15 运营者采购、使用的网络产品和服务，尤其是网络关键设备、网络安全专用产品，应符合法律、行政法规的规定和相关国家标准的强制性要求。

4.4 检测评估

4.4.1 运营者应根据检测评估策略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、方式方法、周期、人员组织、资金保障等。

4.4.2 运营者应自行或者委托网络安全服务机构对其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。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。运营者应将检测评估结果和整改情况及时上报安全保护工作部门。

4.4.3 运营者新建或改建、扩建关键信息基础设施后，应委托安全保护工作部门认可的网络安全服务机构进行检测评估，在对发现的安全问题进行有效整改后方可上线。

4.4.4 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 运营者应根据监测预警策略制定监测预警制度，明确监测内容和流程，采取有效技术措施，实施持续性监测，对关键信息基础设施的网络安全风险进行感知、监测。

4.5.2 安全监测的内容应包括但不限于漏洞利用攻击监测、间谍软件监测、病毒蠕虫攻击监测、木马后门攻击监测、异常流量监测、敏感信息泄露监测。

4.5.3 运营者应按照安全保护工作部门网络安全监测预警和信息通报的要求，建立关键信息基础设施的预警信息响应处置程序。

4.5.4 运营者在收到预警信息后，应按照预警信息响应处置程序，进行分析、研判和处置反馈。

4.5.5 运营者应按照安全保护工作部门网络安全监测预警和信息通报的要求，做好与安全保护工作部门、研究机构、网络安全服务机构的网络安全信息共享工作，共享信息包括但不限于漏洞信息、威胁信息、最佳实践、前沿技术等。

4.6 应急处置

4.6.1 运营者应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，制定本单位的网络安全事件应急预案。应急预案应包括启动应急预案的条件、应急处理流程、系统恢复流程、事件报告流程、事后教育和培训等内容。应对关键信息基础设施网络安全应急预案定期进行评估修订，每年至少组织1次应急演练。

4.6.2 运营者应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。

4.6.3 运营者应制定灾难恢复计划，确保关键信息基础设施能及时从网络安全事件中恢复，并建立安全事件追溯机制。

4.6.4 在网络安全事件发生后，运营者应按应急预案进行处置；事件处置完成后及时向安全保护工作部门书面报告事件情况，内容应至少包括：事件描述、原因和影响分析、处置方式等信息。

4.6.5 运营者对关键信息基础设施中的重要系统和数据应采取GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》中的三级及以上要求进行处置。

4.6.6 运营者应积极参与和配合国家网信部门、安全保护工作部门开展的网络安全应急演练、应急处置等工作。

4.6.7 运营者应根据检测评估、监测预警中发现的安全问题及处置结果开展综合评估，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，乙方承担保密义务的甲方信息包括但不限于以下内容：

(1) 技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；
(2) 业务信息：同甲方业务相关的人员、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：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。

A.2 保密义务

A.2.1 乙方明确所接收的保密信息及其载体均为甲方所有。乙方承认甲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，乙方应当考虑甲方的利益并对该信息予以妥善保管。

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

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

(1) 技术信息：同甲方业务相关的程序、代码、流程、方法、文档、数据等内容；
(2) 业务信息：同甲方业务相关的人员、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：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。

A.2.4 若第三方要求披露甲方敏感信息时，乙方不应响应，并应立刻将情况通告甲方。

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，乙方应返还甲方本协议中规定的信息和甲方数据。所有由甲方提供给乙方的材料，

包括但不限于文件、设计和清单应仍为甲方的财产，且甲方要求时应立即归还原件和所有据此制作的副本。

A.3 违约责任

乙方承认并明确同意：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甲方损失是难以用金钱来衡量的。因此，当乙方出现任何违约情形时，甲方有权要求乙方立即返还相关保密信息，且乙方有义务立即采取合理补救措施。同时，乙方还应赔偿：

(1) 因乙方违约行为，而使甲方遭受的全部经济损失（包括直接损失和间接损失）；

(2) 甲方因调查乙方的违约行为、采取补救措施而支出的所有合理费用（包括但不限于甲方向乙方及第三方追索、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乙方在本协议下就终止生效日前提供给乙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] GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南
[2] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
[3] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南
[4] 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
[5] GB/T 32924-2016 信息安全技术 网络安全预警指南
[6] Framework for Improving Critical Infrastructure Cybersecurity
[7] NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations