

附件 3

《网络关键设备安全技术要求 通用要求 (报批稿)》编制说明

一、工作简况

(一) 任务来源

根据国家标准化管理委员会发布《关于下达〈车用乙醇汽油〉等 13 项强制性国家标准制修订计划的通知》(国标委发〔2019〕26 号)，工业和信息化部负责组织制定《网络关键设备安全技术要求 通用要求》标准项目。

经全国信息安全标准化技术委员会、全国通信标准化技术委员会推荐，综合考虑专家权威性和代表性，工业和信息化部成立了由 21 名专家组成的《网络关键设备安全技术要求 通用要求》标准起草专家组(以下简称标准起草组)。

标准起草组组长由中国互联网协会专家担任，成员包括中国信息通信研究院、国家信息技术安全研究中心、中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、国家工业信息安全发展研究中心、威尔克通信实验室等检测机构，以及华为、联想、中兴、新华三、烽火、和利时、浪潮、浙江中控、深信服、阿里巴巴、中国移动、启明星辰等企业的专家。

(二) 主要工作过程

标准编制主要经历立项、起草、征求意见、技术验证、意见处理、技术审查等环节，具体如下：

1. 立项起草

1) 2018 年 9 月 13 日：工业和信息化部向国家标准化管理委员会报送了《网络关键设备安全技术要求 通用要求》强制性国家标准计划项目建议。

2) 2018 年 9 月-2019 年 8 月：工业和信息化部组织技术检测机构、网络关键设备生产企业、网络安全企业等开展标准预研工作。

3) 2019 年 8 月 31 日：国家标准化管理委员会正式下达《网络关键设备安全技术要求 通用要求》标准项目制定计划，计划号 20192423-Q-339。

4) 2019 年 10 月 25 日：工业和信息化部组织召开标准起草组成立暨项目启动会。

5) 2019 年 12 月 3 日：标准起草组召开第一次工作组会议，形成标准草案。

6) 2019 年 12 月 26 日：标准起草组召开第二次工作组会议，对标准草案进行充分讨论并完善，形成征求意见稿。

2. 征求意见

1) 2020 年 1 月-4 月：工业和信息化部书面征求包括中央网信办等有关部门，中国电信、中国联通、国家电网、平安保险、一汽、华为、中兴、新华三、思科、瞻博、上海贝尔诺基亚、戴尔、西门子、国际商用机器（IBM）、施耐德、罗克韦尔、三菱、欧姆龙等相关企事业单位，以及中国信息通信研究院、国家信息技术安全研究中心、国家计算机网络应急技术处理协调中心等检测机构在内的 60 家单位意见。

2) 2020年3月18日：标准起草组组织中国公司银行、中国电力科学研究院、哈尔滨工程大学、中科院信工所、中汽研、奇安信、360等重点行业单位、企业、社会团体、高校专家召开专题研讨会。

3) 2020年3月30日：标准起草组组织西门子、施耐德、罗克韦尔、浙江中控、和利时、南大傲拓等PLC设备生产厂商召开专题研讨会。

3. 技术验证

2020年3月16日-4月3日：标准起草组组织联想、中兴、和利时、新华三等设备厂商以及中国信息通信研究院、威尔克通信实验室等检测机构开展标准技术要求试验验证工作。标准验证覆盖了路由器、交换机、服务器和PLC设备四类已列入第一批目录的网络关键设备。根据标准验证参与各方反馈，标准条款适用性和可操作性总体良好。对于适用性和可操作性存在不足的技术内容，标准起草组对相关条款进行了修改完善。

4. 意见处理

1) 2020年3月6日：标准起草组召开第三次工作组会议，讨论通过对征求意见的处理意见并修改完善标准。

2) 2020年4月1日：标准起草组召开第四次工作组会议，讨论通过对征求意见的处理意见并修改完善标准。

3) 2020年4月3日：标准起草组修改完善标准内容，形成送审稿。

5. 技术审查

2020年4月10日，工业和信息化部组织召开了《网络关键设备安全技术要求 通用要求（送审稿）》技术审查会，来自全国通信标准化技术委员会、全国信息安全标准化技术委员会、国家信息中心、中国移动等单位的21位专家对标准进行了技术审查。专家一致同意通过技术审查，并提出7条修改意见。

6. 形成报批稿

2020年4月13日：标准起草组召开第五次工作组会议，全部采纳了技术评审会专家意见，修改完善标准内容，形成报批稿。

二、编制原则

本标准依据GB/T1.1-2009《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。针对网络关键设备的技术特点、安全要求、管理流程等进行分析研究，坚持标准的一致性、先进性和可行性，保证标准的科学性和可操作性，切实提升网络关键设备安全性、设备安全管理工作规范性。

本标准的编制遵循以下原则：

（一）需求主导。本标准的编制充分考虑了网络关键设备实际技术特点，确定了网络关键设备定义，分析梳理了网络关键设备必须具备的安全功能要求，并提出了网络关键设备安全保障要求，可为网络运营者采购网络关键设备提供依据，也适用于指导网络关键设备的研发、测试等工作。

（二）确保通用。本标准规定了网络关键设备应满足的通用安全技术要求。为保障标准内容的通用性，本标准在编

制过程中充分参考借鉴国内外相关安全标准，包括：

1) GB/T 18336-2015 信息技术 安全技术 信息技术安全
性评估准则

2) GB/T 18018-2019 信息安全技术 路由器安全技术要
求

3) GB/T 20011-2005 信息安全技术 路由器安全评估准
则

4) GB/T 21050-2019 信息安全技术 网络交换机安全技
术要求（评估保证级 3）

5) GB/T 21028-2007 信息安全技术 服务器安全技术要
求

6) GB/T 25063-2010 信息技术安全 服务器安全测评要
求

7) GB/T 33008.1-2016 工业自动化和控制系统网络安
全 可编程序控制器（PLC） 第 1 部分：系统要求

8) GB/T 36470-2018 信息安全技术 工业控制系统现场
测控设备通用安全功能要求

9) YD/T 1359-2005 路由器设备安全技术要求——高端
路由器（基于 IPv4）

10) YD/T 1439-2006 路由器设备安全测试方法——高
端路由器

11) YD/T 1906-2009 IPv6 网络设备安全技术要求——
核心路由器

12) YD/T 2045-2009 IPv6 网络设备安全测试方法——

核心路由器

13) YD/T 1629-2007 具有路由功能的以太网交换机设备安全技术要求

14) YD/T 1630-2007 具有路由功能的以太网交换机设备安全测试方法

15) YD/T 2042-2009 IPv6 网络设备安全技术要求——具有路由功能的以太网交换机

16) YD/T 2043-2009 IPv6 网络设备安全测试方法——具有路由功能的以太网交换机

17) 3GPP TS 33.117 通用安全保障要求框架 (Catalogue of General Security Assurance Requirements)

18) ITU-T X.805 端到端通信服务安全框架 (Security Architecture for Systems Providing end-to-end Communications)

(三) 立足实际。标准编制立足网络关键设备相关设备安全技术现状，尽量吸纳成熟技术和已有共识的结论，尽量少涉及有争议的问题和不稳定技术，不涉及应用面狭窄或纯学术性的技术，提取适用性和兼容性更高的安全标准要求。

三、主要内容

本标准按照 GB/T1.1-2009 《标准化工作导则第1部分：标准的结构和编写》起草，通过标准起草组深入研究、广泛征求相关方意见等方式保障标准技术内容的完备性。

本标准主要分为六个组成部分：

（一）范围。明确标准适用范围，即网络关键设备应满足的通用安全技术要求。

（二）规范性引用文件。列举了标准中引用其他文件的清单。

（三）术语与定义。标准第 3 章对网络关键设备等概念进行了定义。

（四）缩略语。标准第 4 章对标准中涉及的缩略语进行了说明。

（五）安全功能要求。标准第 5 章提出了网络关键设备应满足的设备标识安全，冗余、备份恢复与异常检测，漏洞和恶意程序防范，预装软件启动及更新安全，用户身份标识与鉴别，访问控制安全，日志审计安全，通信安全，数据安全及密码要求等 10 方面要求。

（六）安全保障要求。标准第 6 章提出了网络关键设备设计和开发、生产和交付、运行和维护等方面应满足的安全保障要求。

四、其他事项说明

（一）与有关法律、行政法规和其他强制性国家标准的关系

《中华人民共和国网络安全法》第二十三条规定，网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。本标准是支撑落实该款规定的强制性国家标准，与我国的现行法律、行政法规和强制性

国家标准内容协调一致。

（二）配套推荐性标准制定情况

为配合《网络关键设备安全技术要求 通用要求》实施，目前，工业和信息化部已组织相关单位提出 6 项配套推荐性国家标准，包括：

- 1) 《网络关键设备安全技术要求 路由器设备》
- 2) 《网络关键设备安全检测方法 路由器设备》
- 3) 《网络关键设备安全技术要求 交换机设备》
- 4) 《网络关键设备安全检测方法 交换机设备》
- 5) 《信息安全技术 服务器安全技术要求和测评准则》
- 6) 《信息安全技术 可编程逻辑控制器（PLC）安全技术要求和测试评价方法》

（三）与国际标准化组织、其他国家或者地区有关法律法规和标准的对比分析

本标准未等同采用任何国际标准。为保障标准要求的通用性和合理性，标准起草组分析、参考、吸收了部分相关国际标准，主要包括：1) 3GPP TS 33.117 通用安全保障要求框架；2) ITU-T X.805 端到端通信服务安全框架。

（四）重大分歧意见的处理经过和依据

标准起草组通过多种形式、多种渠道进行了充分的意见征集和沟通交流，在标准编制过程中，无重大技术问题的分歧意见，也无重要问题需要说明。

（五）标准自发布日期至实施日期之间的过渡期（以下简称过渡期）的建议及理由

建议本标准的过渡期设置为 3 个月。理由：1）在编制过程中，标准起草组组织相关检测机构和部分设备生产厂商进行了技术验证，保障了标准在发布时具有较好的适用性和可操作性；2）《中华人民共和国网络安全法》已于 2017 年 6 月实施，尽快发布和实施本标准有利于相关法律要求落地。

（六）与实施强制性国家标准有关的政策措施

1）国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017 年第 1 号）

2）国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室《关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）的公告》（2018 年第 12 号）

（七）是否需要对外通报的建议及理由

本标准须向 WTO 通报。理由：根据 WTO《技术性贸易壁垒协定》（TBT）第 5.6 条规定，成员的合格评定程序须向 WTO 通报。

（八）涉及专利的有关说明

本标准不涉及专利问题。

（九）强制性国家标准所涉及的产品、过程或者服务目录

国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017年第1号）明确路由器、交换机、服务器、可编程逻辑控制器（PLC设备）为第一批网络关键设备，并规定了具体参数范围。

标准起草组

2020年4月13日