附件

19项通信行业标准编号、名称及主要内容等一览表

| 序号 | 标准编号 | 标准名称 | 标准主要内容 | 代替标准 | 采标情况 |
| --- | --- | --- | --- | --- | --- |
|  | YD/T 4598.4-2024 | 面向云计算的零信任体系 第4部分：数据保护能力要求 | 本文件规定了面向云计算的零信任体系中数据保护能力要求，包括总体架构、数据保护分场景特性能力要求和通用管理能力要求  本文件适用于供应商在云环境下开发、设计和建设基于零信任理念的数据保护产品或解决方案 |  |  |
|  | YD/T 1729-2024 | 电信网和互联网安全等级保护实施指南 | 本文件规定了电信网和互联网安全等级保护的概念、对象、目标、安全等级划分，以及安全等级保护实施过程中的基本原则，并结合电信网和互联网的生命周期定义了电信网和互联网安全等级保护工作的主要阶段及主要活动  本文件适用于电信网和互联网的安全等级保护工作总体性指导，对具体网络的安全等级保护可参考具体网络的安全防护要求和安全防护检测要求 | YD/T 1729-2008 |  |
|  | YD/T 1731-2024 | 电信网和互联网灾难备份及恢复实施要求 | 本文件给出了电信网和互联网灾难备份及恢复工作的目标和原则，描述了电信网和互联网灾难备份及恢复工作的基本实施方法  本文件适用于电信网和互联网的灾难备份及恢复工作，并且可作为电信网和互联网灾难备份及恢复的总体指导性文件，针对具体网络的灾难备份及恢复可参考具体网络的安全防护要求和安全防护检测要求 | YD/T 1731-2008 |  |
|  | YD/T 1734-2024 | 移动通信网安全防护要求 | 本文件规定了IPv4、IPv6、双栈环境下的移动通信网的安全防护要求，包括业务安全、网络安全、网元设备和基础设施安全、物理环境安全和管理安全等方面  本文件适用于指导移动通信网安全防护工作开展和推进 | YD/T 1734-2009 |  |
|  | YD/T 1735-2024 | 移动通信网安全防护检测要求 | 本文件规定了IPv4、IPv6、双栈环境下的移动通信网的安全防护检测要求，包括业务安全、网络安全、网元设备和基础设施安全、物理环境安全和管理安全等方面  本文件适用于移动通信网安全防护检测工作 | YD/T 1735-2009 |  |
|  | YD/T 2669-2024 | 电信网和互联网第三方安全服务能力评定准则 | 本文件规定了为电信网和互联网提供第三方安全服务的组织应具备的各类安全服务能力  本文件适用于指导第三方评定和认证机构开展第三方安全服务能力的评定，可作为国家有关主管部门开展监督管理、电信运营企业选择第三方服务组织的依据，也可以作为第三方安全服务提供商改进自身能力的指导 | YD/T 2669-2013 |  |
|  | YD/T 6104-2024 | 移动互联网仿冒应用程序的监测与处置接口技术要求 | 本文件规定了移动互联网仿冒应用程序上报、审核、监控、反馈、确认与处置流程中的接口要求  本文件适用于互联网应用程序官方厂家、移动应用商店与仿冒应用程序监测与处置平台间的接口 |  |  |
|  | YD/T 6105-2024 | 移动应用商店恶意程序的监测与处置接口技术要求 | 本文件规定了移动应用商店与移动应用商店安全监测与处置管理平台相关接口的信息报送与结果查询流程  本文件适用于移动互联网恶意程序的监测与处置 |  |  |
|  | YD/T 6106-2024 | 移动互联网恶意程序检测引擎评价指标和方法 | 本文件规范了移动互联网恶意程序检测引擎评价指标体系、评价指标和评价方法  本文件适用于指导对部署于云端或本地服务器的移动互联网恶意程序检测引擎的评价 |  |  |
|  | YD/T 6107-2024 | 病毒和恶意地址黑名单信息共享接口技术要求 | 本文件规定了病毒和恶意地址黑名单信息共享接口的技术要求，并定义了对应平台相关接口的接口流程和消息上报格式  本文件适用于病毒和恶意地址黑名单样本的共享与处置 |  |  |
|  | YD/T 6108-2024 | 网络安全威胁数据报送接口要求 | 本文件规定了网络安全威胁数据的内容、数据结构、文件格式，以及报送威胁数据所使用的自动报送接口通信协议  本文件适用于网络安全威胁等数据的自动化报送 |  |  |
|  | YD/T 6109-2024 | 网络深度包检测（DPI）数据密码应用技术要求 | 本文件规范了网络深度包检测（DPI）数据密码应用技术要求，包括网络DPI数据的密码应用总体需求、密码应用流程、密码应用功能要求和安全管理要求  本文件适用于网络DPI数据密码应用相关的方案制定、系统研发、应用实施等 |  |  |
|  | YD/T 6110-2024 | 安全芯片非入侵式攻击缓解测试方法 | 本文件规定了安全芯片非入侵式攻击缓解测试方法，包括安全芯片非入侵式攻击缓解的测试要求、测试准备、测试方法与量化指标、以及特殊情况说明等  本文件适用于指导安全芯片的非入侵式攻击缓解测试，从攻击与测试两个角度为厂商提供安全芯片的设计参考 |  |  |
|  | YD/T 6111-2024 | 对防火墙进行管理的网络功能虚拟化编排器（NFVO）技术要求 | 本文件规定了对防火墙进行管理的网络功能虚拟化编排器（NFVO）相关技术要求，包括技术架构、功能要求等内容  本文件适用于网络功能虚拟化编排器（NFVO）技术研发、设备研制、网络建设和系统运维 |  |  |
|  | YD/T 6112-2024 | 5G移动通信网络设备安全保障要求 核心网网络功能（第二阶段） | 本文件规定了5G移动通信网络中核心网网络功能（第二阶段）安全保障要求，包括第二阶段新增的核心网网络功能及已有网元新增安全需求的安全保障目标、需求、测试内容和测试方法  本文件适用于5G核心网网络功能的安全测试 |  |  |
|  | YD/T 6113-2024 | 面向行业的5G网络通用安全能力技术要求 | 本文件规定了面向行业的5G网络通用安全能力要求，包括业务安全要求、网络安全要求、物理环境安全要求及管理安全要求  本文件适用于面向行业提供安全能力的5G网络，可为垂直行业和5G运营商提供安全指导 |  |  |
|  | YD/T 6114-2024 | 量子密钥分发（QKD）网络 安全技术要求 | 本文件规定了量子密钥分发（QKD）网络的安全技术要求，包括QKD网络的安全威胁框架、安全要求、安全措施、安全等级保护等  本文件适用于量子密钥分发网络规划、设计、建设、运营等 |  |  |
|  | YD/T 6115-2024 | 移动智能终端卫星定位能力技术要求和测试方法 | 本文件规定了移动智能终端卫星定位能力的技术要求以及测试方法，主要包括北斗独立定位、单北斗定位，以及北斗优先定位的功能要求、性能要求和测试方法  本文件适用于支持卫星定位的移动智能终端的设计、研发和测试，包括智能手机、平板电脑、笔记本电脑、可穿戴设备等 |  |  |
|  | YD/T 6116.1-2024 | 算力互联互通能力要求 第1部分：总体框架 | 本文件给出了算力互联互通体系的总体框架，包括算力互联互通的需求、流程机理，同时还规定了算力互联互通的关键能力要求及算力互联互通参考架构以及各个角色之间的关系  本文件适用于算力互联互通体系建设参考 |  |  |