中国质量检验协会文件

中检办发〔2026〕11号

中国质量检验协会关于《未来网络战略安全架构设计　第1部分：总体要求》团体标准征求意见的通知

各有关单位和相关专家：

中国质量检验协会（以下简称本协会）批准立项的《未来网络战略安全架构设计　第1部分：总体要求》团体标准经过有关专家和参编单位讨论和修改，据此形成上述团体标准征求意见稿。

按照《中国质量检验协会团体标准管理办法》的相关规定和要求，本协会现对上述团体标准公开征求意见，请各有关单位和相关专家对上述团体标准制定的修改意见和建议于2026年2月11日前反馈至本协会；如逾期未作反馈，则视为无意见和建议。

谨此感谢有关专家和参编单位与社会各界对本协会团体标准制修订工作的大力支持！

本团体标准编制工作组　联系人：王中生

手机：13032973171

邮箱：wzhsh1681@163.com

中国质量检验协会碳中和绿色发展专业委员会 联系人：蔺枫

电话：010-59196500　　手机：13601123186

邮箱：zwh@chinatt315.org.cn

附件：1.《未来网络战略安全架构设计　第1部分：总体要求》（征求意见稿）

2.团体标准征求意见表

中国质量检验协会

2026年1月12日

ICS
CCS

团　体　标　准

T/CAQI XXXX—XXXX

未来网络战略安全架构设计
第 1 部分 总体要求

Future network strategic security architecture design: Part 1 General requirement

征求意见稿

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

中国质量检验协会　　发 布

目　　次

前　　言 7

引　　言 8

1 范围 9

2 规范性引用文件 9

3 术语和定义 9

4 缩略语 11

5 总则 12

5.1 设计原理 12

5.2 设计原则 12

5.3 设计目标 12

6 要素体系 12

6.1 安全哲学体系 12

6.2 安全指标体系 12

6.3 安全评估体系 13

6.4 安全政策体系 13

6.5 安全管理体系 13

6.6 安全标准体系 13

6.7 安全技术体系 13

6.8 安全设施体系 13

6.9 安全运营体系 13

6.10 安全应用体系 13

6.11 安全创新体系 13

6.12 安全人才培养体系 14

6.13 网络安全服务体系 14

7 系统架构 14

7.1 未来网络安全系统构成 14

7.2 地址安全系统 14

7.3 域名安全系统 14

7.4 自治域安全系统 14

7.5 解析安全系统 14

7.6 传输安全系统 14

7.7 管理安全系统 14

7.8 应用安全系统 14

7.9 经济安全系统 15

7.10 设备安全系统 15

7.11 密码服务系统 15

8 网络安全体系与架构设计要求 15
8.1 安全理论体系设计要求 15
8.2 安全防御体系设计要求 15
8.3 主动隐形防御体系设计要求 15
8.4 递归互连网络体系结构的安全评估要求 15
8.5 安全标准国际化要求 15
8.6 管治体系架构设计要求 16
9 网络安全领域与层级设计要求 16
9.1 主权安全设计要求 16
9.2 国家安全设计要求 16
9.3 运行安全设计要求 16
9.4 社会与经济安全设计要求 16
9.5 平滑演进与过渡期安全设计要求 16
9.6 特定技术选型安全设计要求 17
10 网络结构资源安全设计要求 17
10.1 拓扑结构设计要求 17
10.2 关键基础设施 17
10.3 骨干网设计要求 17
10.4 核心资源设计要求 17
10.5 地址格式设计要求 17
10.6 域名系统设计要求 17
10.7 国家域名与根服务解析设计要求 18
10.8 路由与自治域设计要求 18
10.9 支撑系统设计要求 18
11 区域性与循环网络安全设计要求 18
11.1 总体架构原则 18
11.2 国家内循环网络设计要求 18
11.3 国际及区域性互联设计要求 18
11.4 地方及边缘循环网络设计要求 18
11.5 边界安全设计要求 19
11.6 安全外网架构设计安全 19
11.7 网络演进与迁移安全要求 19
12 技术应用安全设计要求 19
12.1 通用安全设计原则 19
12.2 密码技术应用要求 19
12.3 移动通信网络安全要求 19
12.4 超限通信设计要求 19
12.5 人工智能应用安全要求 19
12.6 物联网安全要求 20
12.7 云计算与边缘计算网络安全要求 20
12.8 特定场景通信网络安全要求 20
12.9 前沿技术安全设计要求 20

13 网络安全应急与特殊应用设计要求 20
13.1 总体韧性设计要求 20
13.2 应急与保底通信架构设计要求 20
13.3 关键基础设施与产业链安全设计要求 20
13.4 重点行业领域安全设计支撑要求 21
14 规划与评估 21
14.1 安全评估通用准则 21
14.2 架构设计方案的评估要求 21
14.3 实用性评估要素 21
参 考 文 献 22

前　言

本文件是《未来网络战略安全架构设计》系列标准的第1部分。系列标准组成如下：

第1部分：总体要求；

第2部分：总体技术方案评估规则；

第3部分：总体技术架构；

第4部分：实施指南。

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》起草。

本文件某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由西安工业大学和吉林省吉规全域数据科技产业研究院有限责任公司提出。

本文件由中国质量检验协会归口管理。

本文件起草单位：西安工业大学、吉林省吉规全域数据科技产业研究院有限责任公司、新型网络与检测控制国家地方联合工程实验室、全域数据信息安全重点联合实验室、全域数据信息安全重点联合实验室泰州战略发展实验室、上海十进制网络信息科技有限公司、南京博丰通信科技有限公司、北京邮电大学、东南大学苏州研究院、香港未来网络标准化研究院、吉林省纵横软件开发有限公司、北京神州天才科技有限公司、江苏图码信息科技有限公司、昆明理工大学、西安工商学院、西北农林科技大学、深圳市伟科未来网络科技有限公司、西安微九网络科技研究院有限公司、厦门市星谷卫星技术应用研究院、北京数立通科技有限责任公司、新疆维吾尔自治区数字经济联合会、克拉玛依职业技术学院、重庆域六名物联网科技有限公司、北京北斗弘鹏科技有限公司、江苏君立华域信息安全技术股份有限公司、金城信息技术安全有限公司、矩阵时光数字科技有限公司、杭州数通科技有限公司、北京神州同正科技有限公司、南京信息工程大学沃特福德学院、陕西华太盾信息安全有限公司、湖州米欧康电子科技有限公司、深圳前海和大数据网络科技有限公司、四川优加溯源科技有限公司。

本文件主要起草人：王中生、赖一阳、谢建平、王建国、李一楠、丁益民、于红芹、杨宝林、余　鲲、吴含前、闫伟宁、李宏光、张家乐、王同超、楼培德、王玉汴、侯　悦、楚晓明、张　琳、刘斌、卜锦华、王艾城、魏红梅、韩　浚、杨兆勇、王　强、李　京、范晓明、孙军豹、文瀚唯、陈　辉、龚莆巽、金建军、唐荣喜、陈增兵、陈国平、赵伟时、陈　周、张红彬、梁　鋆、梁　鉴、王保卫、芦天亮、张彦平、魏　军、蒋永生、曹莜娟、胡丹、胡志成、丁峤、李雨晨、李元杰、孙继烈、张庆松。

本文件为首次发布。

引　言

随着数字和信息技术革命的深入推进，计算机网络已成为事关国家安全和生存权利的关键基础设施，传统网络安全架构在应对人工智能、物联网、云计算、边缘计算等新技术场景，特别是高级别持续性威胁（APT）、零日漏洞等风险时，其主动防御与韧性抗毁能力存在不足。当前，由于缺乏统一的安全架构设计标准，不同厂商与机构采用的网络安全方案难以实现跨域协同防护。特别是在缺乏网络底层架构、核心协议等关键技术及自主权的情况下，现有网络体系难以抵御国家级、有组织、高强度的网络攻击。

为从根本上提升网络安全能力，构建自主可控的未来网络技术体系，并将其打造为支撑经济社会发展与国家安全的战略性基础设施。我国在此领域已进行长期布局，自原信息产业部于 2001 年组织十进制网络技术研究以来，相关成果已在 ISO/IEC 未来网络国际标准体系的核心技术领域贡献了中国方案。国家“十四五”规划、《网络安全法》、“十五五”规划等顶层设计，均为未来网络的发展与安全建设提供了明确的战略指引和政策依据。

为指导未来网络安全技术的研发与应用，支撑国家网络安全防御体系建设，构建基于主权原则的安全稳定网络空间，参考 GB/T 25070、GB/T 38561 等相关国家标准，规定了未来网络战略安全架构的总体设计要求。

本标准主要适用于电力、金融、交通、能源等关键信息基础设施的规划、建设与运营单位，可为网络安全设备厂商与系统集成商提供技术开发依据，为各级政策法规制定、安全评估及行业监管提供统一参考。

本标准实施的目标是：

a) 构建自主可控的未来网络及保障体系，提供系统的设计标准与方法；

b) 通过体系化的安全架构设计，有效降低国家级、有组织、高强度网络攻击的风险；

c) 通过底层架构的安全冗余设计，大幅提升关键信息基础设施的韧性抗毁能力；

d) 促进安全方案的标准化，降低跨系统、跨平台运维难度与成本，增加用户的网络选择。

未来网络战略安全架构设计 第1部分：总体要求

1 范围

本标准规定了未来网络战略安全架构设计的总体原则、构成要素、系统架构以及核心设计要求。

本标准适用于指导未来网络战略安全架构的规划、设计、实施、运营与评估，适用于构建新一代自主可控网络体系。

2 规范性引用文件

下列文献对于本标准的制定是必不可少的。凡是注明日期的引用文件，仅该日期的版本适用于本标准。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 25070-2019 信息安全技术，网络安全等级保护设计技术要求

GB/T 38561-2020 信息安全技术，网络安全管理支撑系统技术要求

ISO/IEC TR 29181-1:2012 信息技术 未来网络 问题陈述和需求 第1部分：概述 (Information technology—Future Network—Problem statement and requirements — Part 1: General Aspects)

ISO/IEC TR 29181-2:2014 信息技术 未来网络 问题陈述和需求 第2部分：命名与寻址 (Information technology—Future Network—Problem statement and requirements — Part 2: Naming and addressing)

ISO/IEC TR 29181-5:2014 信息技术 未来网络 问题陈述和需求 第5部分：安全 (Information technology—Future Network—Problem statement and requirements — Part 5: Security)

ISO/IEC TR 27033-7:2023 信息技术 网络安全 网络虚拟化安全指南 第7部分 (Information technology—Network security Guidelines for network virtualization security — Part 7)

3 术语和定义

GB/T 25070、GB/T 38561界定的以及下列术语和定义适用于本标准。

3.1

未来网络 Future Network

基于空杯设计和全新架构理念与方法，旨在独立于现有因特网体系之外设计和构建的下一代计算机网络体系。注：该概念源自ISO/IEC主导的国际标准化项目。

3.2

未来网络 2.0 Future Network 2.0

在未来网络基础架构理念之上，通过核心机制优化与能力增强，重点提升传输确定性、资源调度效率及内生安全能力的新型网络体系。

3.3

战略安全 Strategic Security

为保障国家根本利益、长远发展与全局稳定，防范和化解可能颠覆国家主权、中断发展进程、动摇生存根基的系统性风险形态。

3.4

战略安全架构 Strategic Security Architecture

为维护战略安全，防范系统性风险而构建的分层分类、协同联动、动态适配的系统性框架。

3.5

空杯设计 Clean State Design

摒弃现有网络体系约束，基于全新架构理念与目标需求进行系统性设计的方法。

3.6

结构性安全 Structural Security

通过构建多层次、全流程、可校验的底层架构与规则体系，从根源上规避安全风险，保障系统、设施或产品在全生命周期内的稳定与可靠。

3.7

网络主权 Network Sovereignty

国家主权在网络空间的自然延伸，指国家对其领土范围内的网络基础设施、网络活动、网络数据及网络治理所享有的独立管辖权和控制权。

3.8

十进制网络 Decimal Network

以全数字地址编码为核心机制的新型网络体系，涵盖地址标识、分配方法及相关的硬件与软件系统。

注：该技术体系已纳入ISO/IEC未来网络国际标准的技术选项范畴，参见SJ/T 11604-2016。

3.9

网络安全架构设计 Network Security Architectural Design

围绕业务与系统需求，构建融合安全域、技术防护、管理流程与应急响应的一体化多层防护体系，以实现网络全生命周期的风险管控。

3.10

确定性网络技术 Deterministic Network Technology

通过网络资源预留、虚拟实电路、路径调度与时钟同步等机制，为特定数据流提供可保证的端到端时延、抖动及丢包率等服务质量（QoS）的网络技术。

3.11

网络空间 Network Space

由互联互通的计算机系统、通信网络、数据资源、虚拟环境以及相关参与主体构成的全球性数字领域。也被称为第五疆域。

3.12

零信任架构 Zero Trust Architecture

一种网络安全模型，其核心是不默认信任网络内部或外部的任何主体，需基于先验证后通讯、持续验证和最小权限授予进行访问控制。

3.13

韧性抗毁网络 Resilient Network

具备在遭受攻击、故障或灾难时，维持关键功能、快速恢复及自适应调整能力的网络。

3.14

隐形攻击 Stealth Attack

一种隐蔽性强、旨在规避常规检测手段的网络攻击方式，攻击者通过伪装、潜伏、利用未知漏洞等手段，窃取数据或破坏系统。

3.15

主动隐形防御 Active Stealth Defense

一种主动网络安全防御策略，通过部署诱骗环境、动态隐藏真实资产、混淆攻击者探测路径等手段，增加攻击者识别和攻击真实目标的难度。

3.16

安全外网 Secure External Network

通过安全隔离、访问控制、入侵防护及地址加密传输等技术加固，实现内、外网安全隔离与合法访问，抵御外部恶意攻击的外部互联网络。

3.17

超限通信网络 Over Limit Communication Networks

采用先进调制、编码与信号处理技术，以实现超越传统信道容量理论极限的通信系统。

3.18

多标识网络 Multi Identifier Network

通过分离身份、内容与位置等多种标识，并建立解析映射关系，以重构网络基础通信模型的网络体系。

3.19

中华公网 Chinese Public Network

基于未来网络（3.1）架构设计理念，核心技术自主可控、体现网络主权（3.7）的新一代国家公众互联网络。

3.20

字符路由 Character Based Routing

依据网络地址中的特定字符序列进行匹配，以确定数据包处理逻辑或转发路径的路由机制。

3.21

物理隔离网络 Physical Separated Network

通过断开物理链路连接、单独部署设备与传输介质，使内部网络与外部网络完全隔绝，拒绝非授权数据交互的网络安全模式。

3.22

保底通信 Default Communications

在常规通信网络瘫痪或失效时，依托卫星、无线自组网、中继等独立于地面基础设施的备用手段，保障关键信息传输与基本通信能力的冗余通信机制。

3.23

过渡期 Transition Period

从现有网络体系向新型网络体系迁移，直至新型网络完全承担主导作用的阶段。

4 缩略语

下列缩略语适用于本标准。

IEC：国际电工委员会（International Electrotechnical Commission）

ISO：国际标准化组织（International Organization for Standardization）

IP：因特网协议（Internet Protocol）

MIN：多标识网络（Multi Identifier Network）

OID：对象标识符（Object Identifier）

RINA：递归互连网络架构（Recursive Interconnection Network Architecture）

SDN：软件定义网络（Software Defined Network）

SLA：服务等级协议（Service Level Agreement）

TCP：传输控制协议（Transmission Control Protocol）

5 总则

5.1 设计原理

a) **改良加固**：作为过渡路径，通过优化配置、增强组件、补充防护等技术措施，系统性提升现有网络的安全性、稳定性与可靠性；

b) **底层创新**：通过对网络底层架构与核心协议进行原创性设计，构建自主可控、内生安全的网络技术体系，从根源上消除结构性安全风险，维护网络主权。

5.2 设计原则

a) **空杯设计**：采用不受现有网络协议约束的全新架构理念进行设计，并通过兼容性创新实现与现有网络的互联互通；

b) **系统自治**：将未来网络架构视为可独立运行、自成体系的有机整体，确保其在不依赖外部网络条件下的生存与运转能力；

c) **顶层统筹**：基于国家战略安全保障需求，进行全局性、前瞻性的整体规划，统筹性能、安全、可扩展性与成本等多维目标；

d) **开放协作**：遵循国际通用规范与安全准则，通过国际合作推进技术标准协同与跨境安全联防联控，保障全球互联互通的稳定与合法流通；

e) **平滑演进**：设计应兼顾技术前瞻性与历史兼容性，支持网络架构、资源与能力的平滑过渡与可持续演进；

f) **内生安全**：将安全能力内嵌于网络底层架构与核心协议中，实现主动防御与动态弹性；

g) **智能管控**：支持基于人工智能的一体化安全态势感知、策略协同与自动化响应。

5.3 设计目标

a) **捍卫网络主权**：通过自主可控的底层架构与核心资源管理，为维护国家网络空间主权提供技术基石；

b) **保障战略安全**：构建能有效抵御国家级、有组织、高强度网络攻击的网络安全防御体系；

c) **构建可信架构**：形成具有内生安全性、结构可靠性和韧性抗毁能力的新一代网络基础架构

d) **引领技术发展**：掌握网络架构、命名寻址、路由交换、安全机制等核心技术的自主知识产权与标准主导权

e) **支撑未来应用**：为全球性新型业务与应用提供安全、可靠、高性能的网络基础设施保障。

6 要素体系

未来网络战略安全架构要素体系由下列十三个相互关联、协同作用的子体系构成。

6.1 安全哲学体系

确立以主动防御、内生安全、协同共生为核心，融合技术理性与价值伦理的网络安全顶层认知与基本范式，指导从被动对抗向主动免疫、从单点防护向生态协同的根本性转变。

6.2 安全指标体系

建立覆盖技术防御、运营管理、治理合规与生态协同等多维度，具备动态量化、风险驱动、韧性优先、业务对齐特性的可测量、可评估、可优化的安全指标集合，以支撑安全态势量化与决策优化。

6.3 安全评估体系

构建融合智能量化、动态实战、全栈覆盖与闭环治理能力的评估机制。该体系应能支撑从事前预测到事后溯源的全链路安全评估，并解决以下核心问题：

a) 安全技术方案的设计方法；
b) 安全技术方案的优劣判定；
c) 安全目标的实现路径验证；
d) 标准一致性与完整性的保障。

6.4 安全政策体系

构建贯穿法律、标准、监管、治理与国际合作的制度框架，遵循发展与安全并重、动态适配、协同共治的原则，为网络空间可信、可控、可持续发展提供政策保障。

6.5 安全管理体系

建立战略、架构、运营、人才与合规协同的治理机制，依托智能驱动与闭环运营，实现对组织、技术、供应链的全生命周期风险管控，保障业务连续性与数据安全。

6.6 安全标准体系

规划包含基础共性、技术专项、行业应用及测评验证层级的动态标准框架，核心覆盖等级保护、密码技术、数据安全及零信任等领域，并统筹国内应用与国际接轨需求。

6.7 安全技术体系

集成零信任、量子安全、隐私计算、云原生安全等关键技术，形成具备主动防御、智能检测、自动响应与持续进化能力的闭环技术能力，保障从终端、数据到业务的全链路安全。

6.8 安全设施体系

按照基础设施层、智能中枢层、应用适配层与实战验证层的分层架构进行部署，并通过集中化运营实现设施联动与策略统一调度，支撑纵深防御与全局协同。

6.9 安全运营体系

构建统一中枢、智能分析、自动化响应与实战验证的一体化运营架构，实现威胁情报联动、告警降噪、自动化处置与跨组织协同，支撑风险驱动的安全运营。

6.10 安全应用体系

通过安全能力模块化封装与自动化编排，实现安全服务按需调用与跨场景协同交付，保障各类上层应用在复杂威胁环境下的安全可信。

6.11 安全创新体系

建立从理论创新、原型验证、工程化落地与实战迭代的转化机制，并配套人才培养与国际化协同机制，以持续培育安全创新能力与产业生态。

6.12 安全人才培养体系

构建政、产、学、研协同的生态化培养路径，建立涵盖学历教育、职业培训、实战历练与终身学习的全链条机制，分层培育战略型、领军型、工程型及技能型网络安全人才。

6.13 网络安全服务体系

建立以标准化安全能力组件为基础，通过需求适配、服务编排、交付运维与持续优化闭环，面向最终用户提供覆盖终端、云端、数据及供应链等全场景的一体化安全服务。

7 系统架构

7.1 未来网络安全系统构成

未来网络安全系统架构应由地址安全、域名安全、自治域安全、解析安全、传输安全、管理安全、应用安全、经济安全、设备安全等子系统及密码服务系统协同构成。

7.2 地址安全系统

设计并采用具有自主知识产权、体现内生安全特性的全新地址格式与体系，确保地址资源的自主可控与安全可靠，从底层支撑网络主权。

7.3 域名安全系统

建立自主可控的新型域名体系或命名机制，确保域名资源的分配、解析与管理安全，并满足国家网络主权维护目标。

7.4 自治域安全系统

制定自主的自治域编码协议与管理规范，在提供网络标识与路由指引的同时，支持国家对网络秩序与资源的安全治理。

7.5 解析安全系统

若采用解析体系，应确保根服务器或核心解析节点的安全可控，可采用去中心化、多机制互补等创新架构以增强解析服务的抗毁性与可信性。

7.6 传输安全系统

通过架构与协议创新，实现信息传输的确定性、高可靠性及内生安全性，提供低时延、抗干扰、防窃密的可靠传输能力。

7.7 管理安全系统

建立覆盖地址、域名、解析、设施、设备及策略的全生命周期安全管理制度与流程，从管理层面保障网络系统的整体安全。

7.8 应用安全系统

为承载于未来网络之上的各类应用提供统一的安全接口与保障机制，支撑应用业务的平滑迁移与安全可信运行。

7.9 经济安全系统

在架构设计中体现提升网络经济效益、降低对外技术依赖成本的理念，并通过可量化的测算方法进行评估。

7.10 设备安全系统

推动基于未来网络协议与安全体系的核心软硬件（如芯片、操作系统、网络设备）的自主研发与安全性能提升，降低关键供应链依赖风险。

7.11 密码服务系统

全面应用国产商用密码算法，构建全链路密码防护体系，并前瞻性部署抗量子密码迁移方案。

8 网络安全体系与架构设计要求

8.1 安全理论体系设计要求

a) 对现有网络架构性缺陷与安全威胁进行全面、深入分析；
b) 为所有架构性与技术性安全解决方案提供原理性支撑；
c) 阐明设计的战略目标、核心特点及其对维护国家主权、安全和发展利益的作用；
d) 保持持续演进的能力，以适应新的安全形势与技术需求。

8.2 安全防御体系设计要求

a) 维持核心业务韧性。能够在面对国家级、有组织、高强度的网络攻击时，保障内循环网络的关键业务平稳运行；
b) 保障战略通道安全。具备在战时等特殊状态下维持关键国际网络通道畅通的能力；
c) 贯彻核心安全原则。落实最小特权、纵深防御与安全措施可验证性原则；
d) 实现全局态势协同。建立基于未来网络架构的全域安全态势感知与情报共享系统。

8.3 主动隐形防御体系设计要求

a) 能力内置。将应对隐形攻击的能力内生于网络架构设计之中；
b) 技术标准化。开发并标准化防范与消除隐形攻击的针对性技术；
c) 体系动态化。构建具有内生安全能力的动态防御体系，实现向主动免疫、动态内生范式的转变；
d) 零信任融合。依据零信任理念，实现“先验证，后通信”的标准化安全接入；
e) 全栈覆盖。防护范围应覆盖从物理层到应用层等网络各层次。

8.4 递归互连网络体系结构的安全评估要求

a) 评估RINA架构对国家网络安全需求的符合性；
b) 分析其与本标准提出的未来网络架构的兼容性与潜在冲突；
c) 验证本标准中安全设计方案在RINA架构下的可实现性；
d) 识别其扁平化等架构特性可能引入的额外安全风险。

8.5 安全标准国际化要求

a) 以推动成为ISO/IEC国际标准为目标；

b) 优先保障国内部署应用，服务国家网络安全战略；
c) 在提炼普适性技术要求构成国际基础框架的同时，可依据国情保留特定安全增强要求；
d) 将中国贡献的国际密码算法等自主技术纳入国际标准选项。

8.6 管治体系架构设计要求

a) 国际治理层。遵循联合国宪章、国际标准与公约等；
b) 国家法规层。依据国内法律、政策及强制性标准；
c) 政府执行层。明确国家层面的管理机构与职能；
d) 公益组织层。依托研究机构与标准化组织支撑；
e) 关键设施运营层。由授权国有大型企业负责建设与运营；
f) 产业生态层。向社会开放，推动全产业链协同发展。

9 网络安全领域与层级设计要求

9.1 主权安全设计要求

a) 遵循并贯彻国家网络主权原则，通过技术落实网络主权；
b) 确保地址、域名、核心路由等关键网络资源的分配、管理权自主可控；
c) 通过创新的底层架构设计，建立独立自治网络空间能力，支撑司法管辖的技术实现；
d) 架构上明确网络空间边界，具备对数据跨境流动进行有效管控的技术能力；

9.2 国家安全设计要求

a) 满足或超过网络安全等级保护第四级和第五级的防护要求；
b) 针对国家级、有组织、高强度的网络攻击进行针对性架构设计，并支持常态化的实战化攻防验证机制；
c) 关键基础设施的架构、设备与供应链安全应符合国家相关审查与管理要求。

9.3 运行安全设计要求

a) 运营须经国家授权，并与外部网络（如因特网）实现有效的安全隔离；
b) 建立并实施覆盖用户、设备、系统的精细化最小权限管理模型；
c) 防止数据非法出境，境内流量非必要不绕转境外；
d) 建立完整的运行安全审计与事件及时上报机制。

9.4 社会与经济安全设计要求

a) 提升基础网络服务的可靠性与韧性，降低大规模断网停服对社会运行造成的风险；
b) 与应急通信、保底通信体系进行架构融合与能力协同；
c) 在架构设计中考虑提升经济效益、降低对外依赖成本的技术路径；
d) 为数据资产的合规流通与安全利用提供架构支撑。

9.5 平滑演进与过渡期安全设计要求

a) 提供从现有网络向未来网络迁移的应用与数据安全兼容方案；
b) 迁移方案应该具有无缝衔接，尊重用户灵活选择网络接入的设计要求，不要为用户进行应用迁移带来过重的负担；

c) 采用足够大的地址空间方案，为技术长期演进提供基础资源保障；
d) 制定并部署过渡期的专项安全增强措施与应急部署方案。

9.6 特定技术选型安全设计要求

a) 软件定义网络。应对其远程控制风险、供应链及与核心安全机制的兼容性进行严格评估与设计；
b) 确定性网络。作为提升路由确定性、时效性及安全性的核心设计领域，推动新型确定性路由协议（如字符路由）的标准化；
c) 等级保护适配。基于未来网络全新架构，研究制定或适配相应的网络安全等级保护制度与实施指南。

10 网络结构资源安全设计要求

10.1 拓扑结构设计要求

a) 综合分布式与集中式结构的优势，形成兼容协同的混合架构；
b) 支持构建国家内循环网络，实现核心业务流量的本地化与可控流转；
c) 支持构建符合国际标准与协作需求的跨境网络交换拓扑。

10.2 关键基础设施

a) 设备采购与运营应符合国家网络安全审查要求；
b) 采用内生安全机制与技术，防范设备被非法控制、干扰与破坏；
c) 建立多源备份与动态切换的供应链保障体系，防范供应中断风险；
d) 部署数据分类分级、全链路加密与精细化访问控制，防范核心数据泄露与非法出境；
e) 通过架构与策略确保关键信息基础设施及核心数据的主权可控。

10.3 骨干网设计要求

a) 与现有网络实现有效安全隔离，并通过兼容机制进行合规信息交换；
b) 核心软、硬件应实现自主可控；
c) 实现全域覆盖并具备冗余备份，形成国家关键基础设施的韧性备份；
d) 规划、部署与运营方案应获得国家主管部门批准。

10.4 核心资源设计要求

a) 具备原创性与自主知识产权；
b) 进行整体规划，预留充足的扩展空间，满足长期演进需求；
c) 所有权、分配权与管理权应确保国家主体掌控；
d) 积极推动其方案纳入国际标准体系。

10.5 地址格式设计要求

a) 采用自主设计的新型地址格式，并确保地址资源的自主分配与管理；
b) 采用大地址空间方案（如默认256位并预留扩展能力），满足可持续发展需求；
c) 兼容可变长度地址等灵活机制，并设计地址压缩与安全功能；
d) 提供地址加密与隐私保护机制。

10.6 域名系统设计要求

a) 建立自主可控的新型域名体系或命名机制；
b) 可创新采用数字域名等方案，并解决其易用性问题；
c) 具备安全的域名查询与解析机制。

10.7 国家域名与根服务解析设计要求

a) 采用国际标准认可的国家代码（如CHN、156、86等）；
b) 根解析服务应境内部署、自主可控，并纳入最高等级安全防护；
c) 管理规则应符合国家法规。

10.8 路由与自治域设计要求

a) 支持分布式、韧性路由架构（如“八纵八横”模式）；
b) 贯彻“先认证，后通信”与“本地优先”的安全路由原则；
c) 满足内循环网络与物理隔离网络的特定路由需求；
d) 自治域系统应实现自主可控，具备内生安全架构，并支持配套的寻址与路由协议。

10.9 支撑系统设计要求

a) 网络授时系统。建立自主可控、高精度、高安全的网络时间同步协议与根服务器体系，并兼容主流国际协议；

b) 数据主权维护。通过网络拓扑（内循环）、路由策略（确定性路由）、地址格式（地理编码）及边界管控等技术机制，为数据跨境流动提供可管控的架构支撑；

c) 物理隔离网络。基于未来网络架构提供高性能、可扩展的新型物理隔离网络解决方案，并强化针对“跨网入侵”等威胁的防御能力。

11 区域性与循环网络安全设计要求

11.1 总体架构原则

未来网络安全架构设计应支持多层次、可协同的网络循环体系，在保障国家网络主权与核心数据安全的前提下，实现可管控的开放互联段建设双循环网络规划。

11.2 国家内循环网络设计要求

a) 流量本地化。坚持国内业务流量境内路由与交换，避免非必要跨境绕转的原则；
b) 资源自治。实现国内网络地址、域名等核心资源的自主解析与管理；
c) 管控能力。在架构上支持对数据出境进行有效识别、审计与管控的技术能力。

11.3 国际及区域性互联设计要求

a) 标准与协作。互联架构与协议应遵循国际标准，并支持多边安全协作机制；
b) 受控通道。通过专用的安全网关或通道进行互联，并对跨境流量实施安全检查和策略控制；
c) 韧性保障。保障在对抗环境下关键国际通信通道的可用性与安全性。

11.4 地方及边缘循环网络设计要求

a) 分层自治。支持省、市、县、园区等多级分层网络自治域；
b) 本地优先。支持“本地优先”路由策略，满足边缘计算的低时延要求；

c) 统一管控。各层级网络应接受国家骨干网的统一策略管控，不得阻碍全域互联互通。

11.5 边界安全设计要求

a) 关口节点。在国际互联处设立安全关口节点，作为实施安全策略的实体；
b) 防御纵深。关口节点应具备深度包检测、入侵防御和抗分布式拒绝服务攻击等能力；
c) 态势溯源。记录并保存跨境安全事件日志，支持攻击溯源与取证。

11.6 安全外网架构设计安全

a) 强隔离性。与企业或机构内部网络实现逻辑或物理隔离；
b) 主动防御。应集成主动隐形防御、流量混淆等高强度安全技术；
c) 可管可控。其接入、访问和数据处理应处于集中化安全管理的控制之下。

11.7 网络演进与迁移安全要求

网络架构设计应支持从现有网络向未来网络的平滑演进，并确保演进过程中的安全，具体要求见本标准相关章节。

12 技术应用安全设计要求

12.1 通用安全设计原则

a) 自主可控。应优先采用并通过国产密码算法、自主可控的硬件与基础软件实现核心安全功能；
b) 架构融合。安全能力应与网络层、计算层及应用层架构进行一体化设计与深度融合；
c) 演进兼容。设计应具备前瞻性，支持向后量子密码等新一代安全技术的平滑演进。

12.2 密码技术应用要求

a) 必须遵循国家商用密码管理政策与标准；
b) 优先采用国产商用密码算法作为默认选项；
c) 支持向后量子密码算法的迁移能力。

12.3 移动通信网络安全要求

a) 实现无线接入、核心网、传输网的全链路安全防护，重点保障空口与信令安全；
b) 保障用户数据在跨网（未来网络与移动网络）传输过程中的机密性、完整性与可控性；
c) 支持天地一体化场景下的统一身份认证与安全管控。

12.4 超限通信设计要求

a) 未来网络要与超限通信技术密切联合，信息通信方式互为补充；
b) 推动超限通信技术在未来网络的应用，形成超限网络技术及应用体系；
c) 未来网络要与超限通信技术一起在新一代公共安全体系发挥作用，如应急通信、保底通信、终端直连卫星通信等；
d) 未来网络的安全架构设计应该为这些新型通信网络提供更可靠的安全保障。

12.5 人工智能应用安全要求

a) 保障训练数据、模型参数及推理过程在传输与计算中的机密性与完整性；

b) 实现基于最小权限和动态信任的模型与数据访问控制；
c) 具备针对数据投毒、模型窃取、对抗样本等特定攻击的防护与检测能力；
d) 确保人工智能的决策与操作处于人类监督与安全策略的最终控制之下。

12.6 物联网安全要求

a) 实现海量异构终端设备的统一、轻量级身份认证与准入控制；
b) 保障从终端、边缘到云端全链路数据的机密性与完整性；
c) 支持设备行为异常监测与协同响应。

12.7 云计算与边缘计算网络安全要求

a) 实现多租户间严格的数据隔离与安全策略隔离；
b) 保障计算任务与数据在中心云与边缘节点之间安全调度与协同；
c) 边缘节点自身应具备轻量化的抗物理篡改与入侵检测能力。

12.8 特定场景通信网络安全要求

a) 卫星及空间通信。实现空天地一体化网络的安全协议兼容与统一管控，优先采用北斗系统提供授时与定位服务；
b) 车联网。支持基于“本地优先”路由和边缘计算的车路协同低时延安全通信，保障车联网数据主权；
c) 工业控制网络。支持与物理隔离网络、确定性网络技术的深度结合，保障生产控制指令的实时性与安全性；
d) 区块链。应用区块链技术，网络层设计应保障共识机制安全与智能合约的可靠执行环境。

12.9 前沿技术安全设计要求

a) 对未来前沿技术的安全集成保持关注并预留能力；
b) 对量子通信与计算技术保持关注并预留能力；
c) 对超限通信等新型调制编码技术保持关注并预留能力。

13 网络安全应急与特殊应用设计要求

13.1 总体韧性设计要求

a) 未来网络架构应具备内生韧性，以满足特殊场景下的安全需求；
b) 支持核心业务在遭受攻击、故障或灾害时的持续运行与快速恢复；
c) 采用分布式、冗余和可重构的架构，避免单点故障，并能动态隔离威胁；
d) 实现安全策略与网络状态的动态适配与自动化响应。

13.2 应急与保底通信架构设计要求

a) 应急、救灾、保底等极端场景的通信网络具有抗毁性能；
b) 采用多制式融合、多路径冗余的架构，确保在基础网络损毁时的连通性；
c) 建立独立或逻辑强隔离的网络通道，实施端到端加密与严格的身份认证与权限控制；
d) 支持不依赖地面固定基础设施的快速部署组网能力。

13.3 关键基础设施与产业链安全设计要求

a) 供应链透明可信。建立对关键软硬件组件的来源、完整性和安全性的验证机制；
b) 深度防御。结合网络、系统、数据、应用等多层次防护，并与物理安全措施协同；
c) 业务连续性保障。通过架构设计降低单点供应中断对核心业务的影响。

13.4 重点行业领域安全设计支撑要求

a) 未来网络架构应为金融、能源、电力、交通等重点行业提供可定制的安全设计支撑；
b) 支撑构建满足行业最高安全等级要求的逻辑或物理隔离网络环境；
c) 提供低时延、高可靠、确定性路径的安全传输能力，支撑工业控制、金融交易等业务；
d) 在架构层面提供精细化的数据分类、标记与跨境流动管控能力。

14 规划与评估

14.1 安全评估通用准则

a) 对象界定。聚焦符合未来网络基本特征、不依赖现有因特网基础架构的自主技术体系；
b) 层级优先。遵循体系、架构、具体技术的层级顺序，优先考察整体安全体系的完备性与协调性；
c) 创新导向。将自主创新作为评估的核心要素与基本前提，重点考察其对提升国家网络安全的实质贡献；
d) 风险审查。对引入非自主来源的技术，必须进行严格的安全威胁分析，并确保其经过安全性改造与可控集成。

14.2 架构设计方案的评估要求

a) 完整性。以未来网络整体体系为支撑，安全设计应为有机组成部分；
b) 先进性。评估方案是否代表全新设计范式，及其对安全性、性能带来的实质性改善；
c) 可比性。对多个备选方案，应基于统一的评估指标和基准环境进行公平对比分析。

14.3 实用性评估要素

a) 演进路径。应评估其技术发展路径与分阶段实施的可行性；
b) 平滑演进。应评估过渡期内安全保障的策略，以及与现有网络兼容互通的迁移方案；
c) 符合性基础。该体系应能为开发产品认证、测评规范等符合性评估活动提供技术依据。

参 考 文 献

[1] 国家标准化管理委员会，等. 关于印发《关于实施公共安全标准化筑底工程的指导意见》的通知: 国标委联〔2024〕23号 [Z]. 2024.

[2] ISO/IEC TR 29181-1:2012 Information technology — Future Network — Problem statement and requirements — Part 1: General Aspects [S].

[3] ISO/IEC TR 29181-2:2014 Information technology — Future Network — Problem statement and requirements — Part 2: Naming and addressing [S].

[4] ISO/IEC TR 29181-5:2014 Information technology — Future Network — Problem statement and requirements — Part 5: Security [S].

[5] ISO/IEC TR 27033-7:2023 Information technology — Network security — Guidelines for network virtualization security — Part 7: Guidelines for network virtualization security [S].

[6] NIST. SP 800-207 Zero Trust Architecture [S/OL]. (2020-08). https://doi.org/10.6028/NIST.SP.800-207

[7] 李　挥，　等. 多边共管多标识网络：体系及技术[M]. 北京：　科学出版社，　2021.

[8] 王中生，　谢建平. 十进制网络技术与应用[M]. 北京：　电子工业出版社，　2021.

[9] ITU-T. X.1056 : Security framework for network resiliency [S]. 2021.

附件 2

团体标准征求意见表

单位名称或 专家姓名			单位盖章或 专家签名	
联系人			联系方式	
标准名称		未来网络战略安全架构设计 第 1 部分：总体要求		
序号	章节	修改意见		具体理由
备注：修改意见和具体理由，可另附相关说明				

本团体标准编制工作组联系人：王中生，手机：13032973171，邮箱：wzhsh1681@163.com。

抄送：本协会会员工作部，本协会存档（2）。

中国质量检验协会　　2026年1月12日印发