

全国网络安全标准化技术委员会秘书处

网络安全标准化工作月报

2026 年第 6 期（总第 53 期）

2026 年 7 月

本期目录

国家标准研制.....	1
1. 1 项强制性网络安全国家标准、13 项规范类指导性技术文件计划下达.....	1
2. 39 项网络安全国家标准公开征集参编单位.....	1
3. 7 项网络安全国家标准获批发布.....	1
4. 4 项推荐性国家标准公开征求意见.....	2
5. 41 项网络安全国家标准正式立项.....	2
6. 召开 10 项网络安全国家标准专家审查会.....	2
7. 63 项网络安全国家标准复审工作.....	2
国际标准化推进.....	3
1. 完成 3 项国际标准文件投票和评议工作.....	3
重要会议.....	3
1. 6 项人工智能应用安全国家标准化指导性技术文件启动会在京召开.....	3
标准实施应用.....	5
1. 开展《网络安全标准实践指南——工业企业数据安全能力成熟度模型》应用推广工作.....	5
标准化文件.....	5
1. 《智能体部署使用安全指引》1 项网络安全标准实践指南发布.....	5
2. 《半导体存储介质块擦除技术指引》等 6 项网络安全标准实践指南征求意见稿公开征求意见.....	6
附件 1: 2026 年 7 月在研国家标准项目推进工作一览表.....	7
附件 2: 2026 年 7 月国际标准文件投票和评议工作一览表.....	10

▽ 国家标准研制

1.1 项强制性网络安全国家标准、13 项规范类指导性技术文件计划下达

7 月 1 日，国家标准化管理委员会下达的指导性技术文件计划中，《网络安全技术 攻击面管理实施指南》等 13 项指导性技术文件由全国网安标委归口管理。7 月 2 日，强制性国家标准制修订计划中，《智能体应用安全基本要求》1 项强制性国家标准委托全国网安标委制定。秘书处分别向各工作组、各项目牵头承担单位印发下达国家标准计划的通知，请项目所属工作组制定项目推进计划，督促项目牵头承担单位按计划抓紧落实，加强协调，广泛征求意见，确保标准质量和水平，按要求完成国家标准制修订任务。

2.39 项网络安全国家标准公开征集参编单位

7 月，秘书处根据《标准参与单位管理办法》，对密码技术、鉴别与授权、网络安全评估、通信安全、网络安全管理、数据安全、新技术安全、人工智能安全领域等 39 项网络安全国家标准公开征集参编单位。

3.7 项网络安全国家标准获批发布

7 月 7 日，根据国家市场监督管理总局、国家标准化管理

理委员会发布的《中华人民共和国国家标准公告》（2026 年第 30 号），由全国网络安全标准化技术委员会归口的《网络安全技术 网络安全产品互联互通 第 4 部分：威胁信息格式》等 7 项国家标准正式发布。

4.4 项推荐性国家标准公开征求意见

7 月 15 日，《网络安全技术 SM9 标识密码算法 第 2 部分：算法》《信息技术 安全技术 匿名实体鉴别 第 4 部分：基于弱秘密的机制》《数据安全技术 数据提供、委托处理、共同处理实施指南》《网络安全技术 人工智能应用安全分类分级方法》等 4 项推荐性国家标准征求意见稿面向社会公开征求意见，征求意见期限为 60 天。

5.41 项网络安全国家标准正式立项

7 月 16 日，全国网安标委发布《关于 2026 年 41 项网络安全国家标准项目立项的通知》。

6.召开 10 项网络安全国家标准专家审查会

7 月 16 日，秘书处组织召开《政务信息系统网络安全基本要求》《人工智能安全能力成熟度评估方法》等 10 项标准征求意见稿专家审查会。

7.63 项网络安全国家标准复审工作

7月20日，秘书处公布对63项国家标准复审工作结论，其中继续有效50项、修订13项，并于7月17日上报国家标准委。

▽ 国际化推进

1. 完成3项国际标准文件投票和评议工作

2026年7月，秘书处共组织完成ISO/IEC 29128-2《信息安全 网络安全和隐私保护 密码协议验证 第二部分：密码协议的评估方法和活动》、ISO/IEC 27045.2《信息安全 网络安全和隐私保护 大数据安全和隐私 大数据风险管理指南》、ISO/IEC 27014《信息安全 网络安全和隐私保护 信息安全治理》等3项国际标准文件投票和评议工作。

▽ 重要会议

1. 6项人工智能应用安全国家标准化指导性技术文件启动会在京召开

为贯彻落实《加快推动人工智能百项国家标准建设专项行动计划》，2026年7月8日，秘书处在北京组织召开6项人工智能应用安全国家标准化指导性技术文件启动会。市场监管总局标准技术司信息技术与自动化标准处处长曹一丁、中央网信办网络安全协调局审查评估处处长范兵出席会议

并作指导讲话。应急管理部科技和信息化司、金融监管总局科技监管司、国家广播电视总局科技司、教育部科学技术与信息化司等有关行业主管部门代表，人工智能安全标准工作组（WG9）副组长张震，以及6项指导性技术文件编制组代表共30余人参加会议。会议由中国电子技术标准化研究院网络安全研究中心主任姚相振主持。

会上，《网络安全技术 人工智能应用安全 卫生健康》《网络安全技术 人工智能应用安全 广播电视》《网络安全技术 人工智能应用安全 教育》《网络安全技术 人工智能应用安全 应急管理》《网络安全技术 人工智能应用安全 金融》《网络安全技术 人工智能应用安全 政务》6项技术文件的编制组代表分别汇报了编制思路和工作计划。与会人员围绕6项技术文件的研制思路、编制体例、主要内容、时间节点等方面进行了深入交流讨论。

本次启动会的召开为6项指导性技术文件研制工作搭建了高效的跨部门沟通协调平台，有助于统一编制思路、明确时间节点和质量要求，进一步凝聚行业共识，强化责任分工，为后续标准文本起草、征求意见和审查报批等各环节工作的顺利推进奠定了坚实基础。

▽标准实施应用

1. 开展《网络安全标准实践指南——工业企业数据安全能力成熟度模型》应用推广工作

为贯彻落实《中华人民共和国数据安全法》《网络数据安全条例》《工业和信息化领域数据安全管理办法（试行）》中相关要求，引导工业企业逐级提升数据安全能力成熟度水平，带动数据安全技术、产品和服务在工业企业的落地应用，7月27日，秘书处发布“关于开展《网络安全标准实践指南——工业企业数据安全能力成熟度模型》应用推广工作的通知”，计划选取一批重点行业工业企业依据标准实践指南开展评估工作，对标准实践指南内容的可操作性和适用性进行验证，探索形成实施应用工作模式，提升我国工业企业数据安全能力水平。

▽标准化文件

1. 《智能体部署使用安全指引》1项网络安全标准实践指南发布

7月1日，秘书处组织编制的《网络安全标准实践指南——智能体部署使用安全指引》发布。该实践指南给出了评估、准备、部署、使用、停用等阶段的智能体部署使用安全

指引，适用于智能体部署使用的安全风险防范，也可供选择使用商业智能体服务提供参考。

2. 《半导体存储介质块擦除技术指引》等 6 项网络安全标准实践指南征求意见稿公开征求意见

7 月 3 日，为配套 GB 46864-2025《数据安全技术 电子产品信息清除技术要求》强制性国家标准落地实施，指导相关单位规范开展信息清除活动，秘书处组织编制了《半导体存储介质块擦除技术指引》《电子产品信息清除记录、标识与回收管理指引》《移动智能终端信息清除技术指引》等 3 项网络安全标准实践指南征求意见稿，并于 7 月 2 日至 7 月 17 日面向社会公开征求意见。

7 月 24 日，为指导网络数据处理者、第三方机构在开展网络数据安全风险评估等工作过程中，与其他评估、审计、认证结果的互相采信，秘书处组织编制了《网络数据安全风险评估采信指南》1 项网络安全标准实践指南征求意见稿，并于 7 月 24 日至 8 月 7 日面向社会公开征求意见。

7 月 29 日，为帮助智能体相关服务提供者提升安全水平，防范化解智能体快速发展应用带来的新风险、新挑战，秘书处组织编制了《智能体交互安全要求》《AI 浏览器安全实践指南》等 2 项网络安全标准实践指南征求意见稿，并于 7 月 29 日至 8 月 12 日面向社会公开征求意见。

附件 1：2026 年 7 月在研国家标准项目推进工作一览表

序号	国标计划号	项目名称	标准范围	项目进展
1	20252487-T-469	网络安全技术 工业控制系统安全管理基本要求	本标准从机构、制度、人员、资产和运维等方面提出了工业控制系统的安全管理基本要求；适用于非涉及国家秘密的工业控制系统建设、运行、使用、管理等相关方进行工业控制系统安全管理的规划和落实，也可为工业控制系统安全测评提供参考。	未通过征求意见稿专家审查会，尽快根据专家意见完善文后再次上会。
2	20257064-T-469	网络安全技术 工业控制网络监测安全技术要求及测试评价方法	本标准规定了工业控制网络监测产品的安全技术要求和测试评价方法；适用于工业控制网络监测产品的设计、开发及测评等提供指导，同时也可为工业控制系统设计、建设和运维方开展工业控制系统安全防护工作提供指导。	未通过征求意见稿专家审查会，尽快根据专家意见完善文后再次上会。
3	20260699-T-469	网络安全技术 工业控制系统专用防火墙技术规范	本文件标准了工业控制系统专用防火墙（以下简称工控防火墙）的安全功能要求、自身安全要求、性能要求、安全保障要求，给出了相应的测试评价方法。并提出了安全等级划分要求；适用于工控防火墙的设计、研发、生产、检测和认证。	已通过征求意见稿专家审查会，并于 2026 年 8 月 4 日至 10 月 3 日公开征求意见。
4	20257058-T-469	网络安全技术 具有中央处理器的 IC 卡嵌入式软件安全规范	本标准规范了对具有中央处理器的 IC 卡嵌入式软件达到 EAL4+和 EAL5+安全保障级别所要求的安全功能要求、安全保障要求，以及配套的测试和评估方法；适用于对具有中央处理器的 IC 卡嵌入式软件产品的测试、评估和采购活动，也可用于指导该类产品的研制和开发。	已通过征求意见稿专家审查会，并于 2026 年 8 月 4 日至 10 月 3 日公开征求意见。

序号	国标计划号	项目名称	标准范围	项目进展
5	20257065-T-469	网络安全技术 移动终端安全管理平台技术要求	本标准规定了移动终端安全管理平台的技术要求,包括安全功能要求、自身安全功能要求、安全保障要求及测试评价方法,并提出产品等级划分要求;适用于移动终端安全管理平台产品的设计、开发、检测和认证,为组织实施移动互联应用的安全防护提供参考。移动终端安全管理平台仅针对组织或机构(以下简称“组织”)生产、办公等工作使用的移动智能终端进行安全监测和防护。	已通过征求意见稿专家审查会,并于2026年8月4日至10月3日公开征求意见。
6	20260697-T-469	网络安全技术 政务信息系统网络安全基本要求	本标准规定了政务信息系统的安全总体要求,以及规划设计、建设实施、运行维护等阶段的安全要求;适用于各级党政机关、群团组织以及有关事业单位政务信息系统的安全管理;不适用于涉及国家秘密的政务信息系统。	已通过征求意见稿专家审查会,并于2026年8月4日至10月3日公开征求意见。
7	20261218-T-469	网络安全技术 电子认证安全服务机构运营管理规范	本标准规定了电子认证服务机构认证服务管理、机房建设与运维、认证系统建设与运维、组织与人员管理、信息资产管理、业务连续性要求、审计与评估、法律责任与合规性等要求;适用于在公共网络环境中提供数字证书服务的电子认证服务机构的建设、管理及评估。对于在封闭环境中(如在特定团体或某个行业内)运行的电子认证服务机构可根据自身安全风险评估以及国家有关的法律法规参考本文件。国家有关的测评机构、监管部门也可将本文件作为测评和监管的依据。	已通过征求意见稿专家审查会,尽快完善文本发起公开征求意见。
8	20261219-T-469	网络安全技术 桌面云安全技术要求	本标准规定了基于虚拟化技术的桌面云在应用过程中的安全技术要求;适用于桌面云的安全设计、开发,可用于指导桌面云安全测试。	已通过征求意见稿专家审查会,尽快完善文本发起公开征求意见。

序号	国标计划号	项目名称	标准范围	项目进展
9	20261217-T-469	网络安全技术 云计算服务运行监管框架	本标准确定了云计算服务运行监管框架，规定了安全控制措施监管、变更管理监管和应急响应监管的内容及监管活动，给出了运行监管实现方式的建议；适用于对党政机关、关键信息基础设施运营者使用的云计算服务进行运行监管。	已通过征求意见稿专家审查会,尽快完善文本发起公开征求意见。
10	20262850-T-469	网络安全技术 人工智能安全能力成熟度评估方法	本标准给出了人工智能安全能力成熟度评估模型，确立了数据安全、模型安全、应用安全三类安全对象的安全能力成熟度等级要求及评估方法；适用于对组织在人工智能开发、训练、测试、部署、调用、退役、运营等活动中的安全能力成熟度进行评估，也可作为监管部门对组织提出要求或进行遴选的参考依据。	已通过征求意见稿专家审查会,尽快完善文本发起公开征求意见。

附件 2：2026 年 7 月国际标准文件投票和评议工作一览表

序号	标准编号	英文名称	中文名称	阶段	标准内容
1.	ISO/IEC 29128-2	Information security — cybersecurity and privacy protection — Verification of cryptographic protocols — Part 2: Evaluation methods and activities for cryptographic protocols	信息安全 网络安全和隐私保护 密码协议验证 第二部分：密码协议的评估方法和活动	FDIS	ISO/IEC 29128-2 规范了密码协议在理论上的安全评估方法，包含对协议自动证明器和协议模型（协议应用模型和攻击者模型）的评估方法，协议评估结果可以作为 ISO/IEC 29128 第三部分开展协议实现层面安全评估的输入。
2.	ISO/IEC 27045.2	Information security — cybersecurity and privacy protection — Big data security and privacy — Guidelines for managing big data risks	信息安全 网络安全和隐私保护 大数据安全和隐私 大数据风险管理指南	DIS	ISO/IEC 27045.2 可为大数据生命周期中面临的风险进行识别和应对提供指南，可以用于加强相关组织和机构在大数据安全风险方面的能力。

序号	标准编号	英文名称	中文名称	阶段	标准内容
3.	ISO/IEC 27014	Information security — cybersecurity and privacy protection — Governance of information security	信息安全 网络安全和隐私保护 信息安全治理	FDIS	ISO/IEC 27014 提供了信息安全治理的概念、目标和过程的指南，帮助组织评估、指导、监督和沟通组织内部与信息安全相关的过程。