

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 4 期（总第 51 期）

2026 年 5 月

本期目录

国家标准研制.....	1
1. 28 项网络安全国家标准获批发布	1
2. 1 项网络安全推荐性国家标准计划下达	1
3. 7 项国家标准征求意见稿、8 项国家标准送审稿专家审查	1
国际标准化推进.....	2
1. 完成 5 项国际标准文件投票和评议工作	2
2. 征集 ISO/IEC JTC1/SC27 网络安全国际标准提案	2
标准化文件.....	3
1. TC260-005 《人工智能应用伦理安全指引 1.0》发布	3
附件 1: 2026 年 5 月在研国家标准项目推进工作一览表.....	1
附件 2: 2026 年 5 月国际标准文件投票和评议工作一览表.....	4

▽ 国家标准研制

1. 28 项网络安全国家标准获批发布

根据国家市场监督管理总局、国家标准化管理委员会发布的《中华人民共和国国家标准公告》（2026 年第 21 号、23 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 SM2 密码算法加密签名消息格式》等 28 项国家标准正式发布。

2. 1 项网络安全推荐性国家标准计划下达

2026 年 5 月，国家标准化管理委员会下达的推荐性国家标准计划中，《网络安全技术 网络安全事件管理第 4 部分：协同》1 项国家标准由全国网安标委归口管理。5 月 9 日，秘书处分别向各工作组、各项目牵头承担单位印发《关于下达 16 项网络安全推荐性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，在计划执行中要加强协调，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。

3. 7 项国家标准征求意见稿、8 项国家标准送审稿专家审查

5 月 26 日、5 月 27 日，秘书处组织《网络安全技术 SM9 标识密码算法 第 2 部分：算法》《网络安全技术 关键信息

基础设施安全测评要求》等 7 项网络安全国家标准征求意见稿和《网络安全技术 区块链共识机制安全要求》《数据安全 数据安全保护要求》《网络安全技术 政务云平台安全监测方法》等 8 项网络安全国家标准送审稿专家审查。与会专家围绕标准主要技术内容、意见处理情况进行了审查，并提出修改意见。

▽ 国际标准化推进

1. 完成 5 项国际标准文件投票和评议工作

2026 年 5 月，秘书处共组织完成 ISO/IEC 27017《信息安全 网络安全和隐私保护 基于 ISO/IEC 27002 的云服务信息安全控制》、ISO/IEC 27000《信息安全 网络安全和隐私保护 信息安全管理体系 概述》、ISO/IEC 4922-3《信息安全 安全多方计算 第 3 部分：基于混淆电路的机制》、ISO/IEC 27566-3《信息安全 网络安全和隐私保护 年龄保证系统 第 3 部分：分析或比较方法》、ISO/IEC 31700-3《消费者保护 消费品和服务设计的隐私 第 3 部分：消费品和服务设计的隐私审计》等 5 项国际标准文件投票和评议工作。

2. 征集 ISO/IEC JTC1/SC27 网络安全国际标准提案

5 月 8 日，为继续推进我国网络安全国际标准化工作，

鼓励更多网络安全技术和应用领域优秀实践经验以及科研项目标准成果向国际输出，网安标委秘书处现组织开展 SC27 国际标准提案征集工作，面向网络安全领域产学研用等相关单位征集提案，提案优先但不限人工智能安全、数据安全、个人信息保护、密码算法、物联网安全、关键信息基础设施安全、供应链安全等我国具有技术优势和丰富实践应用经验等领域。

征集截止日期为 2026 年 5 月 29 日，秘书处将按照《网络安全国际标准化活动管理办法》有关评审程序进行审查后，遴选出符合要求的提案，上报国家标准委。

标准化文件

1. TC260-005 《人工智能应用伦理安全指引 1.0》发布

5 月 19 日，在 2026 年中国网络文明大会人工智能赋能网络文明建设分论坛上，网安标委发布了《人工智能应用伦理安全指引 1.0》（以下简称《指引》）。

为进一步引导人工智能应用坚持以人为本、智能向善，推动人工智能应用相关方正确认识和妥善应对应用活动中的伦理安全影响，促进人工智能应用在规范有序、安全可控的轨道上健康发展，《指引》给出了人工智能应用伦理安全理念与原则，明确了人工智能应用开发、服务提供和应用使

用等安全指引。

《指引》的发布，正是对引导人工智能应用尊重人的主体地位、维护公平正义、保障合法权益、促进社会信任，推动人工智能技术始终朝着有益、安全、公平方向发展这一时代课题的积极回应，体现了人工智能治理坚持积极稳妥、开放包容、协同共治的实践导向，也体现了网络文明建设对人工智能时代技术向善、价值引领和秩序塑造的主动回应。

▽附件 1：2026 年 5 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	20257073-T-469	网络安全技术 SM9 标识密码算法 第 2 部分：算法	本标准规定了 SM9 标识密码算法中数字签名算法、密钥交换协议、密钥封装机制和公钥加密算法；适用于 SM9 标识密码算法工程化的实现，指导 SM9 标识密码算法相关产品的研制和检测。	已通过征求意见稿专家审查会，根据专家意见完善文本后尽快发起公开征求意见。
2	20260698-T-469	网络安全技术 匿名实体鉴别 第 4 部分：基于弱秘密的机制	本标准规定了基于弱秘密的匿名实体鉴别机制、每种机制的具体操作步骤以及详细的输入输出；适用于服务器在无法获取可用来识别用户具体身份信息的情况下对用户进行校验，确认其属于特定用户群组的场景。	已通过征求意见稿专家审查会，根据专家意见完善文本后尽快发起公开征求意见。
3	20252484-T-469	网络安全技术 物联网感知终端应用安全技术要求	本标准规定了应用感知终端过程中的安全技术要求，覆盖物联网规划设计、建设、运维管理和废弃退出各阶段；适用于物联网建设运维单位对感知终端的选取、部署、使用维护、废弃等活动，也可以为感知终端产品设计和制造提供指导，为第三方测评机构实施测试和评价提供参考。	已通过送审稿专家研讨会，根据专家意见完善文本后提请全体委员审议。
4	20252486-T-469	网络安全技术 可信计算规范 服务器可信支撑平台	本标准确立了服务器可信支撑平台的总体框架，并规定了服务器可信支撑平台的功能要求及其自身安全要求；适用于服务器可信支撑平台的设计、生产、集成、管理和测试。	已通过送审稿专家研讨会，根据专家意见完善文本后提请全体委员审议。

序号	国标计划号	项目名称	标准范围	项目进展
5	20251312-T-469	数据安全技术 未成年人产品和服务个人信息保护要求	本标准给出了未成年人网络产品和服务的个人信息保护原则和目标、个人信息处理要求、安全保护要求，以及新技术新应用相关的安全要求；适用于未成年人网络产品和服务提供者在开发和运营过程中强化和优化个人信息保护机制，也可检查、评估等活动，以及监护人选用、使用未成年人网络产品和服务提供参考。	已通过送审稿专家研讨会，根据专家意见完善文本后提请全体委员审议。
6	20230248-T-469	数据安全技术 公共数据开放安全要求	本标准规定了公共数据开放过程的安全要求、公共数据开放平台安全要求、公共数据开放动态监测要求和公共数据开放定期评估要求；适用于指导各级政务部门和具有公共管理和服务职能的组织及其技术支撑单位，规范公共数据安全开放，也可为主管部门和第三方机构开展监督管理和评估提供参考。	已通过送审稿专家研讨会，根据专家意见完善文本后提请全体委员审议。
7	20251238-T-469	网络安全技术 政务云平台安全监测方法	本标准描述了政务云平台安全内部监督的通用方法，并分类别描述了具体的检查内容；适用于指导政务云服务商开展内部监督工作。	已通过送审稿专家研讨会，根据专家意见完善文本后提请全体委员审议。
8	20230236-T-469	网络安全技术 关键信息基础设施安全测评要求	本标准提出了针对关键信息基础设施开展网络安全检测和评估的方法；适用于关键信息基础设施运营者及安全检测评估服务机构开展的关键信息基础设施网络安全检测和评估工作。	已通过征求意见稿专家审查会，并于2026年6月17日至8月16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
9	暂无	网络安全技术 人工智能代码生成服务安全要求	本标准规定了人工智能代码生成服务的安全技术要求,以及对应的测试评价方法;适用于人工智能代码生成服务提供者开展服务的安全设计、开发、测试、上线及运维等活动,也适用于第三方评估机构对人工智能代码生成服务进行安全测评。	已通过征求意见稿专家审查会,根据专家意见完善文本后尽快发起公开征求意见。
10	20260951-T-469	网络安全技术 人工智能应用安全分类分级方法	本标准规定了人工智能应用安全分类分级方法,包括原则、框架、步骤和流程等;适用于行业领域主管(监管)部门参考制定本行业本领域的人工智能应用安全分类分级标准规范,也适用于各地区、各部门开展人工智能应用安全分类分级工作,同时为人工智能应用开发者、运营者进行应用安全分类分级提供参考。	已通过征求意见稿专家审查会,根据专家意见完善文本后尽快发起公开征求意见。
11	20260326-T-469	网络安全技术 人工智能技术涉及未成年人应用安全指南	本标准确立了人工智能技术涉及未成年人应用安全的基本原则,提供了人工智能技术涉及未成年人应用在安全需求分析、设计开发、测试验证、部署运营、更新维护和终止运营等阶段的安全指导;适用于人工智能服务提供者向未成年人提供服务时开展未成年人权益保障,也可为监管、检查、评估等活动提供参考。	已通过征求意见稿专家审查会,根据专家意见完善文本后尽快发起公开征求意见。

▽附件 2：2026 年 5 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 27017	Information security — cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services	信息安全 网络安全和隐私保护 基于 ISO/IEC 27002 的云服务信息安全控制	FDIS	ISO/IEC 27017 基于 ISO/IEC 27002，为云服务提供商和云服务客户提供了适用于云服务的信息安全控制实施指南，包含针对云环境的额外控制措施和具体指导。
2.	ISO/IEC 27000	Information security — cybersecurity and privacy protection — Information security management systems — Overview	信息安全 网络安全和隐私保护 信息安全管理体系 概述	FDIS	ISO/IEC 27000 是信息安全管理体系（ISMS）系列的总览和基础词汇文件，阐述了信息安全与 ISMS 的核心概念和原则，并解释了 ISO/IEC 27001 等相关标准之间的关系。

序号	标准编号	英文名称	中文名称	阶段	标准内容
3.	ISO/IEC 4922-3	Information security — Secure multiparty computation — Part 3: Mechanisms based on garbled circuit	信息安全 安全多方计算 第3部分：基于混淆电路的机制	DIS	ISO/IEC 4922-3 作为在研国际标准 ISO/IEC 4922-1《安全多方计算 第1部分：总则》和 ISO/IEC 4922-2《安全多方计算 第2部分：基于密钥共享机制》的第3部分，其核心思想是将两方参与的安全计算函数编译成布尔电路的形式，并将真值表加密打乱，从而实现电路的正确输出而不泄露参与计算的双方私有信息及中间计算结果。
4.	ISO/IEC 27566-3	Information security — cybersecurity and privacy protection — Age Assurance Systems — Part 3: Comparison or Analysis	信息安全 网络安全和隐私保护 年龄保证系统 第3部分：分析或比较方法	CD	ISO/IEC 27566-3 为分析或比较不同类型的年龄保证系统提供了一套结构化的方法与指南，围绕功能性、性能、隐私保护、安全性和可接受性五大核心有效性指标，系统性地描述了分析流程、测试方法、数据收集与结果报告要求。
5.	ISO/IEC 31700-3	Consumer protection — Privacy by design for consumer goods and services — Part 3: Audits of privacy by design for consumer products and services	消费者保护 消费品和服务设计的隐私 第3部分：消费品和服务设计的隐私审计	NP	ISO/IEC 31700-3 规定了一种采用问卷方式对消费品和服务是否符合 ISO 31700-1 高层次要求进行审核的方法，涵盖产品、流程及管理方面，并引入问卷档案法以便对基于附加背景的要求开展审核。除 ISO 19011 所包含的指导外，本文件还就以下方面提供进一步指导：基于 ISO 31700-1 的消费品和服务隐私保护设计审核方案的管理、审核的实施，以及 PCGS 审核员的能力要求。