

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 7 期（总第 54 期）

2026 年 8-9 月

本期目录

国家标准研制.....	1
1. 12 项网络安全国家标准公开征集参编单位	1
2. 12 项推荐性国家标准公开征求意见	1
3. 召开 2 项网络安全国家标准专家审查会	1
4. 48 项网络安全国家标准和 13 项指导性技术文件明确责任专家及责任编辑	2
国际标准化推进.....	2
1. 完成 13 项国际标准文件投票和评议工作	2
2. 2026 年下半年 ISO/IEC JTC1/SC44 工作组会议和全体会议在加拿大蒙特利尔召开	3
重要活动.....	4
1. 全国网络安全标准化技术委员会 2026 年第二次“标准周”活动在济南举办	4
2. “2026 年国家网络安全宣传周——电子产品信息清除分论坛”在济南成功召开	5
重要通知.....	7
1. 个人信息保护标准应用实践案例入选建议名单公示	7
2. 印发关于全国网络安全标准化技术委员会换届及征集委员的	

通知	7
标准化文件.....	7
1. 《人工智能安全治理框架 3.0》发布	7
2. 《个人用户使用人工智能服务安全指南》等 9 项网络安全标准 实践指南发布	8
3. 《智能体系统开发安全指南》1 项网络安全标准实践指南征求 意见稿公开征求意见	9
附件 1：2026 年 8-9 月在研国家标准项目推进工作一览表.....	10
附件 2：2026 年 8-9 月国际标准文件投票和评议工作一览表.....	14

▽ 国家标准研制

1. 12 项网络安全国家标准公开征集参编单位

8 月，秘书处根据《标准参与单位管理办法》，对密码技术、网络安全管理、数据安全、新技术安全、人工智能安全领域等 12 项网络安全国家标准公开征集参编单位。

2. 12 项推荐性国家标准公开征求意见

8 月 4 日、8 月 26 日，《消费类智能联网设备分级要求》《具有中央处理器的 IC 卡嵌入式软件安全规范》《工业控制系统专用防火墙技术规范》《移动终端安全管理平台技术要求》《政务信息系统网络安全基本要求》《移动通信信号屏蔽器技术规范》《工业控制系统安全管理基本要求》《工业控制网络监测安全技术要求及测试评价方法》《网络安全事件管理 第 4 部分：协同》《数据安全能力成熟度模型》《人工智能安全能力成熟度评估方法》

《桌面云安全技术要求》等 12 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。

3. 召开 2 项网络安全国家标准专家审查会

8月21日，秘书处组织召开秘书处组织召开《工业控制系统安全管理基本要求》《工业控制网络监测安全技术要求及测试评价方法》2项标准征求意见稿专家审查会。

4. 48项网络安全国家标准和13项指导性技术文件明确责任专家及责任编辑

8月24日，全国网安标委发布《关于指定48项网络安全国家标准和13项国家标准化指导性技术文件责任专家及责任编辑的通知》。

国际化推进

1. 完成13项国际标准文件投票和评议工作

2026年8-9月，秘书处共组织完成ISO/IEC 25545《网络安全 边缘计算安全与隐私保护指南》、ISO/IEC 27555《信息安全 网络安全与隐私保护 个人可识别信息（PII）删除指南》、ISO/IEC 24843《信息安全 基于属性的凭证》、ISO/IEC 10267《信息技术 数据使用 数据集所含个人信息的量化方法》、ISO/IEC 25093-1《网络安全 机密计算 第1部分：概述和概念》等13项国际标准文件投票和评议工作。

2. 2026 年下半年 ISO/IEC JTC1/SC44 工作组会议和全体会议在加拿大蒙特利尔召开

ISO/IEC JTC1/SC44 工作组会议和全体会议于 2026 年 8 月 31 日至 9 月 3 日以线上线下结合的形式在加拿大蒙特利尔举行,10 个成员国参加了会议。

9 月 1 日为工作组会议,8 月 31 日、9 月 2 日至 3 日为全体会议。工作组会议共讨论了 4 项在研标准项目、1 项标准项目复审、5 项预研工作项目。全体会议听取了工作组及咨询组召集人工作情况汇报,讨论了修改 SC44 标题和范围、取消 AHG1 临时工作组等内容。

全国网安标委组织中国代表团一行 10 人参加了会议,主要取得以下工作成果。一是我国提出的《隐私设计消费者电子产品信息清除功能设计指南》《面向消费者的人工智能智能体隐私设计》和《消费品和服务的隐私设计未成年人保护》3 项预研工作项目(PWI)成功立项;二是推动我国牵头的 ISO/IECPWI26226《隐私增强技术在消费者隐私设计中的应用》进入新工作项目(NP)立项投票阶段;推动我国参与的 ISO/IEC31700-3《消费者保护消费品与服务的隐私设计第 3 部分:消费品与服务隐私设计审计》进入工作组草案(WD)阶段。三是我国专家争取到 SC44 到 IEC/TC124(可穿戴电子设备和安全技术委员会)、IECSycAAL(主动辅助生活系统委员会)2 个联络官职务。

本次会议中国代表团在标准立项和国际组织职务方面双获突破。下一步,网安标委将重点推进新立项项目的技术研究,跟踪在研标准进展,同步储备新提案,持续提升中国在隐私保护国际标准化领域的参与度和影响力。

重要活动

1. 全国网络安全标准化技术委员会 2026 年第二次“标准周”活动在济南举办

9月15日至18日,全国网安标委2026年第二次“标准周”活动在山东省济南市举办。15日上午,“标准周”全体成员会议召开,中央网信办副主任、国家网信办副主任、全国网安标委主任委员王京涛出席并讲话。

会上,受邀专家围绕新一代商用密码算法、网络安全产品互联互通、科学智能(AI4S)安全、具身智能和智能体安全等主题,分享网络安全技术方案和标准化实践。

本次“标准周”活动由全国网安标委主办,中国电子技术标准化研究院承办,中国互联网发展基金会网络安全专项基金支持。全国网安标委副主任委员和委员、秘书长和副秘书长、工作组组长和副组长、成员单位代表,中央网信办网络安全协调局、市场监管总局标准创新管理司和

济南市负责同志共 900 余人参加。期间，组织召开 8 个标准工作组会议、网络安全国际标准研究组会议等。

2. “2026 年国家网络安全宣传周——电子产品信息清除分论坛”在济南成功召开

2026 年 9 月 15 日，由全国网络安全标准化技术委员会秘书处主办，中国电子技术标准化研究院、中国网络安全产业联盟数据安全工作委员会、新一代信息安全与隐私保护标准化技术工业和信息化部重点实验室联合承办的

“2026 年国家网络安全宣传周——电子产品信息清除分论坛”在济南成功举办。中央网信办网络安全协调局副局长屠守中出席会议并发表主题演讲，国家市场监管总局标准创新管理司相关负责同志出席会议，中国电子技术标准化研究院副院长范科峰出席会议并致欢迎词。本次会议由中国电子技术标准化研究院网络安全中心副主任李琳主持。

会议期间，中国电子技术标准化研究院网络安全中心主任姚相振对 GB 46864-2025 实施及国际标准化工作推进情况进行了介绍。会议还邀请了来自中国银行信息科技运营中心、中国资源循环集团电子电器有限公司、华为终端有限公司等行业专家代表，分享了电子产品信息清除功能开发实现、二手电子产品回收过程信息清除实践、金融行业设备退装信息清除标准化解决方案等相关内容。为构建行

业自律的良好生态，推动标准落地实施，会上由中国电子技术标准化研究院牵头，联合中资环电子、联想、小米、小天才、爱回收、转转、中国电子装备技术开发协会等 10 余家生产制造企业、回收平台、第三方机构和组织代表，共同发起了电子产品信息清除行业自律倡议，并发布了电子产品信息清除公共服务平台。

为配套 GB 46864-2025 强标落地实施，指导相关单位规范开展信息清除活动，本次论坛发布并解读了《半导体存储介质块擦除技术指引》《电子产品回收过程中的信息清除管理指引》《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。会上同期开展了以“守护电子产品信息安全与清除实施的关键点和突破口”为主题的圆桌讨论，围绕“强标实施关注重点和已开展相关工作、电子产品及二手流通中信息安全存在的新的卡点堵点、打消消费者隐私顾虑及助力产业能力提升相关建议”等三方面问题进行了详细的交流。

9 月 14 日，2026 年国家网络安全宣传周在济南开幕。电子产品信息清除分论坛作为本届国家网络安全宣传周的重要活动之一，对推动电子产品信息清除技术、标准、产业互动，促进 GB 46864-2025 强标应用实施，以及二手电子产品在全国范围内安全有序流通具有重要作用。

▽重要通知

1. 个人信息保护标准应用实践案例入选建议名单公示

8月11日，按照《关于征集个人信息保护标准应用实践案例的通知》（网安秘字〔2026〕30号），经案例征集、形式审查、技术评审环节，秘书处评选出了入选网络安全国家标准应用实践案例库（个人信息保护主题）的9项案例建议名单并予以公示，公示期为2026年8月12日至19日。

2. 印发关于全国网络安全标准化技术委员会换届及征集委员的通知

9月2日，全国网安标委印发《关于全国网络安全标准化技术委员会换届及征集委员的通知》，根据《全国专业标准化技术委员会管理办法》相关要求，面向重点行业主管部门、地方网络安全主管部门、重点企业、高等院校、科研机构等单位的技术专家或代表，公开征集第四届TC260委员。

▽标准化文件

1. 《人工智能安全治理框架 3.0》发布

9月14日，在国家互联网信息办公室的指导下，全国网安标委组织中国网络空间研究院、国家互联网信息办公室数

据与技术保障中心等专业机构、科研院所、行业企业编制的《人工智能安全治理框架 3.0》在 2026 年国家网络安全宣传周开幕式上发布。

2. 《个人用户使用人工智能服务安全指南》等 9 项网络安全标准实践指南发布

8 月 24 日，秘书处组织编制的《网络安全标准实践指南——个人用户使用人工智能服务安全指南》发布。该实践指南提供了个人用户通过互联网使用人工智能服务的安全指引，包括安全意识提升、安全使用指引、使用行为准则等，可为人工智能服务的技术提供者、服务开发者、服务运营者保障个人用户的安全使用提供参考。

9 月 15 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，秘书处组织编制发布了《半导体存储介质块擦除技术指引》等 3 项网络安全标准实践指南。

9 月 15 日，为有效应对人工智能快速发展应用带来的新风险新挑战，安全释放人工智能应用需求，秘书处组织编制发布了《人工智能应用安全指引 总则》等 4 项网络安全标准实践指南。

9 月 15 日，秘书处组织编制的《网络安全标准实践指南

——个人用户使用人工智能服务安全指南》发布。该实践指南给出了座舱数据处理安全要求，包括安全基本要求、安全技术要求和安全管理要求，适用于座舱数据处理活动，也可作为汽车座舱功能设计研发提供参考。

3. 《智能体系统开发安全指南》1项网络安全标准实践指南征求意见稿公开征求意见

9月18日，为指导智能体系统安全开发，防范化解相关安全风险，秘书处组织编制了《网络安全标准实践指南——智能体系统开发安全指南（征求意见稿）》，并于9月18日至10月2日面向社会公开征求意见。

附件 1：2026 年 8-9 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	20260948-T-469	网络安全技术 消费类智能联网设备分级要求	本标准提出了消费类智能联网设备安全框架和安全定级规则，规定了消费类智能联网设备在物理与硬件安全、系统与软件安全、网络与通信安全、数据与信息安全及安全保障等方面的安全分级要求；适用于消费类智能联网设备安全设计、开发、使用和维护，也适用于第三方机构对消费类智能联网设备进行安全测评；不适用于网络关键设备和网络安全专用产品等特定领域设备。	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。
2	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。
3	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
4	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。
5	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。
6	20261185-T-469	网络安全技术 移动通信信号屏蔽器技术规范	本标准规定了移动通信信号屏蔽器（以下简称屏蔽器）的技术要求和测试方法；适用于移动通信信号屏蔽器的研制、生产和检测。	已通过征求意见稿专家审查会，并于2026年8月26日至10月25日公开征求意见。
7	20262358-T-469	网络安全技术 网络安全事件管理 第4部分：协同	本标准是多组织在协同处理网络安全事件时提供了指南，说明了外部合作对单个组织事件管理的影响，为单个组织协调事件管理过程以及协调小组（如有）开展跨组织事件响应活动提供指导；提出的网络安全事件协同指南是通用的，适用于任何类型、规模或性质的组织，组织可根据其类型、规模与网络安全风险情况相关的业务特性调整指南；也适用于参与合作的单个组织。	已通过征求意见稿专家审查会，并于2026年8月26日至10月25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
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，并于2026年8月26日至10月25日公开征求意见。
9	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，并于2026年8月26日至10月25日公开征求意见。
10	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，也可作为工业控制系统安全测评提供参考。	已通过征求意见稿专家审查会，并于2026年8月26日至10月25日公开征求意见。
11	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，同时也可作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。	已通过征求意见稿专家审查会，并于2026年8月26日至10月25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
12	20257066-T-469	数据安全技术 数据安全能力成熟度模型	本标准确立了由数据安全过程、安全能力、能力成熟度等级构成的数据安全能力成熟度模型，给出了数据安全能力过程域体系，规定了每个能力过程域在各等级、安全能力维度的特征；适用于对组织数据安全能力进行评估，也可作为组织开展数据安全能力建设的依据。	已通过征求意见稿专家审查会，并于2026年8月26日至10月25日公开征求意见。

附件 2：2026 年 8-9 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 25330-1	Information security — Oblivious transfer — Part 1: General	信息安全 不经意传输 第一部分：通用	DIS	ISO/IEC 25330-1 规定了不经意传输数据的密码机制，并提供了不经意传输的术语、通用模型、相关参数及各项要求。
2.	ISO/IEC 25545	Cybersecurity — Guidelines for edge computing security and privacy	网络安全 边缘计算安全与隐私保护指南	NP	ISO/IEC 25545 针对边缘计算资源受限节点、分布式信任域、增加的本地攻击面等特有安全风险，提出基于 ISO/IEC27002 体系的风险控制指南和措施。
3.	ISO/IEC 27555	Information security — cybersecurity and privacy protection — Guidelines on personally identifiable information deletion	信息安全 网络安全与隐私保护 个人可识别信息（PII）删除指南	DIS	ISO/IEC 27555 为各类组织建立和执行个人信息（PII）的删除策略与流程，提供了一个系统化的框架，旨在帮助组织遵循“数据最小化”和“留存限制”等隐私原则，确保 PII 在合法合规的期限内被及时、安全地删除。

序号	标准编号	英文名称	中文名称	阶段	标准内容
4.	ISO/IEC 24843	Information security — Attribute-based credentials	信息安全 基于属性的凭证	CD	ISO/IEC 24843 规定了属性凭证机制的协议构成、功能要求和安全属性，面向数字身份认证中最小披露、匿名使用和不可关联等隐私需求，可弥补传统数字签名需披露完整签名数据、易被跨场景追踪的不足。
5.	ISO/IEC 27004	Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	信息技术 安全技术 信息安全管理 监视、测量、分析和评价	DIS	ISO/IEC 27004 提供了旨在协助组织评估信息安全绩效以及信息安全管理体系有效性的指南，有助于组织满足 ISO/IEC 27001:2022 的 9.1 条款。
6.	ISO/IEC 10267	Information technology — Data usage — Methods to quantify the amount of personal information in a dataset	信息技术 数据使用 数据集所含个人信息的量化方法	DIS	ISO/IEC DIS 10267 用于指导量化个人信息残留量，估算去标识化数据集的个体识别难度，帮助组织机构做好隐私保护与数据合规流转。该文件是原则性指导标准，不支持外部数据场景下的识别难度估算，也不提供个人信息判定方法。
7.	ISO/IEC 25093-1	Cybersecurity — Confidential computing — Part 1: Overview and concepts	网络安全 机密计算 第 1 部分：概述和概念	DIS	ISO/IEC DIS 25093-1 给出了机密计算相关内容，并介绍其核心概念，适用于参与机密计算研发、落地实施或使用的各类机构及相关利益方。

序号	标准编号	英文名称	中文名称	阶段	标准内容
8.	ISO/IEC 19795-1	Information technology — Biometric performance testing and reporting — Part 1: Principles and framework	信息技术 生物特征识别性能测试与报告 第 1 部分：原则与框架	DIS	ISO/IEC DIS 19795-1 规定了生物识别系统性能测试的一般原则、性能指标、测试数据记录和测试结果报告的要求。
9.	ISO/IEC 27115-1	Information security, cybersecurity and privacy protection — Cybersecurity of system of systems — Part 1: Security architecture description	信息安全 网络安全与隐私保护 系统之系统的网络安全 第 1 部分：安全架构描述	CD	ISO/IEC 27115-1 定义了用于构建系统之系统（SoS）安全架构描述的框架，这一部分阐述了如何描述参考或解决方案安全架构的基础，包括实现结构安全和风险评估的方法。
10.	ISO/IEC 25857	Cybersecurity — Guidance for addressing social engineering threats within the digital environment	网络安全 数字环境下社会工程威胁应对指南	NP	ISO/IEC 25857 针对社会工程攻击缺乏系统分类和防护指导国际标准的问题，提出基于攻击生命周期的社会工程威胁分类框架，并针对不同阶段提出相应安全考虑，具有较强的现实需求和国际适用性。
11.	ISO/IEC 27007	Information security — cybersecurity and privacy protection — Guidelines for information security management systems auditing	信息安全 网络安全和隐私保护 信息安全管理体系审核指南	DIS	ISO/IEC 27007 在 ISO 19011 的基础上，对信息安全管理体系（ISMS）审核方案管理、审核实施，以及 ISMS 审核员能力等方面提供了指南。

序号	标准编号	英文名称	中文名称	阶段	标准内容
12.	ISO/IEC 14888-6	Information security — Digital signatures with appendix — Part 6: Stateless hash-based mechanisms	信息安全 带附录的数字签名 第 6 部分：无状态的基于哈希的机制	CD	ISO/IEC 14888-6 规范了无状态的基于哈希的数字签名机制。
13.	ISO/IEC 5181	Information security, cybersecurity and privacy protection — Data provenance	信息安全 网络安全和隐私保护 数据溯源	FDIS	ISO/IEC 5181 给出了数据溯源的原理和方法论，可作为行业做数据溯源的非常基础的理论参考。