

全国信息安全标准化技术委员会秘书处

网络安全标准化工作月报

2023 年第 10 期（总第 26 期）

2023 年 12 月 31 日

本期目录

国家标准研制	1
1. 1 项网络安全国家标准计划下达	1
2. 5 项网络安全国家标准获批发布	1
3. 4 项国家标准征求意见稿专家审查	2
4. 1 项国家标准公开征求意见	2
5. 3 项国家标准送审稿专家审查	2
6. 3 项国家标准送审稿全体委员投票	3
国际标准化推进	4
1. 征集 ISO/IEC JTC1/SC27 网络安全国际标准提案	4
2. 我国牵头提出的 1 项国际标准正式发布	4
3. 完成 5 项国际标准文件投票和评议工作	5
重要会议和活动	5
1. 信安标委 WG1 和工作组组长联席会议在北京召开	5
其他	6
1. 1 项网络安全标准实践指南公开征求意见	6
附件 1: 2023 年 12 月在研标准项目推进工作一览表	7
附件 2: 5 项国际标准文件投票和评议工作一览表	9

▽ 国家标准研制

1.1 项网络安全国家标准计划下达

12月1日，国家标准化管理委员会下达的推荐性国家标准计划中，包括1项由全国信息安全标准化技术委员会归口的标准项目《信息安全技术 网络攻击和网络攻击事件判定准则》。秘书处向工作组、项目牵头承担单位印发《关于下达1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。

2.5 项网络安全国家标准获批发布

根据2023年12月28日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（2023年第20号），信安标委归口的5项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 29246-2023	信息安全技术 信息安全管理体系概述和词汇	GB/T 29246-2017	2024-07-01
2	GB/T 35290-2023	信息安全技术 射频识别（RFID）系统安全技术规范	GB/T 35290-2017	2024-07-01
3	GB/T 43557-2023	信息安全技术 网络安全信息报送指南		2024-07-01

序号	标准编号	标准名称	代替标准号	实施日期
4	GB/T 43577.1-2023	信息安全技术 电子发现 第1部分：概述和概念		2024-07-01
5	GB/T 43578-2023	信息安全技术 通用密码服务接口规范		2024-07-01

3.4 项国家标准征求意见稿专家审查

12月8日、21日，秘书处组织《信息安全技术 信息安全风险管理指导》《信息安全技术 信息安全管理体系 要求》《信息安全技术 网络安全产品互联互通 资产信息格式》《信息安全技术 网络安全产品互联互通 告警信息格式》4项网络安全国家标准征求意见稿专家审查。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。4项标准均通过审查。详见附件1。

4.1 项国家标准公开征求意见

12月4日，《信息安全技术 政务计算机终端核心配置规范》国家标准征求意见稿面向社会公开征求意见，同时秘书处书面发函征求副主任委员单位意见，征求意见期限为60天。详见附件1。

5.3 项国家标准送审稿专家审查

12月8日、21日，秘书处组织《信息安全技术 数据安全风险评估方法》《信息安全技术 大型互联网企业内设个

人信息保护监督机构要求》《信息安全技术 网络攻击和网络攻击事件判定准则》3项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。3项标准均通过审查。详见附件1。

6.3 项国家标准送审稿全体委员投票

12月26日，秘书处组织全体委员对《信息安全技术 办公设备安全规范》《信息安全技术 网络安全产品互联互通框架》《信息安全技术 数据安全评估机构能力要求》3项国家标准送审稿进行投票，全部通过全体委员投票。编制组根据委员意见修改完善后形成标准报批稿。



国际化推进

1. 征集 ISO/IEC JTC1/SC27 网络安全国际标准提案

12月4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，秘书处组织开展 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，提案优先但不限于人工智能安全、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的领域。

征集截止日期为 2023 年 12 月 29 日，秘书处将按照《信息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，上报国标委。

2. 我国牵头提出的 1 项国际标准正式发布

2023 年 12 月，我国牵头提出的 1 项国际标准 ISO/IEC 27033-7:2023 《信息技术 网络安全 第 7 部分：网络虚拟化安全指南》正式发布。

ISO/IEC 27033-7 分析了网络虚拟化的安全挑战，提出了网络虚拟化的安全模型和安全原则，并为网络虚拟化的安全

实施提供指引。该国际标准适用于 5G、算力网络等网络虚拟化场景，可指导相关方防范新型网络环境下的安全风险。

3. 完成 5 项国际标准文件投票和评议工作

2023 年 12 月，秘书处共组织完成 ISO/IEC 9797-2:2021 Cor 1《信息安全 消息鉴别码 第 2 部分：采用专用哈希函数的机制 技术勘误 1》、ISO/IEC 27006-1《信息安全 网络安全和隐私保护 信息安全管理体系审核和认证机构要求 第 1 部分：通用》、ISO/IEC 27017《信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实践规则》等 5 项国际标准文件投票和评议工作，详见附件 2。



重要会议和活动

1. 信安标委 WG1 和工作组组长联席会议在北京召开

12 月 27 日，信安标委 WG1 和工作组组长联席会议在北京召开。会议讨论了《信安标委 2023 年工作总结和 2024 年工作要点(讨论稿)》，审议了《网络安全国家标准体系(2023 版)》，与会专家提出了许多建设性意见和建议。会议对 53 项网络安全国家标准复审结论建议进行了评审，评选形成“2023 年信安标委标准化工作先进个人提名名单”。



其他

1.1 项网络安全标准实践指南公开征求意见

为指导大型互联网平台评估发现和防范可能影响社会稳定、公共利益的网络安全风险，秘书处组织编制了《网络安全标准实践指南——大型互联网平台网络安全评估指南（征求意见稿）》，并于2023年12月23日至2024年1月5日面向社会公开征求意见。

附件 1：2023 年 12 月在研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	20231924-T-469	《信息安全技术 信息安全风险管理指导》	该标准提供指导，以帮助组织满足 GB/T 22080 有关应对信息安全风险活动的要求，实施信息安全风险管理活动，特别是信息安全风险评估和处置；适用于所有组织，无论其类型、规模或领域。	已形成征求意见稿，并通过专家审查会评审。
2	20231925-T-469	《信息安全技术 信息安全管理体系 要求》	该标准规定了在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求，包括了根据组织需求所剪裁的信息安全风险评估和处置的要求；适用于各种类型、规模或性质的组织。	已形成征求意见稿，并通过专家审查会评审。
3	暂无	《信息安全技术 网络安全产品互联互通 资产信息格式》	该标准规定了网络安全产品互联互通资产信息的描述格式；适用于网络安全产品的设计、开发、应用和测试。	已形成征求意见稿，并通过专家审查会评审。
4	暂无	《信息安全技术 网络安全产品互联互通 告警信息格式》	该标准规定了网络安全产品互联互通时告警信息的描述格式；适用于网络安全产品互联互通的设计、开发、应用和测试。	已形成征求意见稿，并通过专家审查会评审。

序号	国标计划号	项目名称	标准范围	项目进展
5	20230238-T-469	《信息安全技术 政务计算机终端核心配置规范》	该标准规定了政务计算机终端核心配置对象、配置范围、配置要求、基线配置描述文件的格式规范、配置的自动化实现方法、实施流程，描述了配置要求对应的证实方法；适用于政务部门开展计算机终端的核心配置工作。	已形成征求意见稿，并于2023年12月4日至2024年2月3日公开征求意见。
6	20230793-T-469	《大型互联网企业内设个人信息保护监督机构要求》	该标准规定了大型互联网企业建立和运行个人信息保护监督机构的要求，包括个人信息保护监督机构的设置、职责、工作规则，以及个人信息保护监督机构的成员等要求；适用于大型互联网企业建立和运行个人信息保护监督机构，也可为监管、检查、评估等活动提供参考。	已形成送审稿，并通过专家审查会评审。
7	20230257-T-469	《信息安全技术 数据安全风险评估方法》	该标准阐述了数据安全风险评估的基本概念、要素关系、分析原理，规定了数据安全风险评估的实施流程、评估内容、分析与评价方法等，明确了数据安全风险评估各阶段的实施要点和工作方法；适用于指导数据处理者、第三方评估机构开展数据安全风险评估，也可供有关主管监管部门实施数据安全检查评估时参考。	已形成送审稿，并通过专家审查会评审。
8	20231460-T-469	《信息安全技术 网络攻击和网络攻击事件判定准则》	该标准确立了网络攻击和网络攻击事件的描述信息要素、判定指标和计数标准；适用于指导组织开展网络攻击和网络攻击事件的监测分析、态势感知、信息报送等活动。	已形成送审稿，并通过专家审查会评审。



附件 2：5 项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 9797-2:2021 Cor 1	Information security — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function — Technical Corrigendum 1	信息安全 消息鉴别码 第 2 部分：采用专用哈希函数的机制 技术勘误 1	CD	该项目由韩国提出，韩国专家担任编辑。ISO/IEC 9797-2 技术勘误 1 对 ISO/IEC 9797-2:2021 标准文本第 4、6、8、9 章及附录 B 的部分数进行了修正。
2.	ISO/IEC 27006-1	Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General	信息安全 网络安全和隐私保护 信息安全管理体系审核和认证机构要求 第 1 部分：通用	FDIS	该项目由德国提出，德国、日本、英国专家担任编辑。ISO/IEC 27006-1 在 ISO/IEC 17021-1 的基础上，对实施信息安全管理体系审核和认证的机构给出了要求和指引。本文件可用于 ISMS 认证机构认可和评审。

序号	标准编号	英文名称	中文名称	阶段	标准内容
3.	ISO/IEC 27017	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实践规则	CD	该项目由日本提出，日本、塞浦路斯专家担任编辑。ISO/IEC 27017 在 ISO/IEC 27002 的基础上，为云计算或云服务组织落实 ISO/IEC 27002 附录 A 中的条款提供实施指南。
4.	ISO/IEC 4922-2	Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing	信息安全 安全多方计算 第 2 部分：基于秘密共享的机制	FDIS	该项目由日本提出，日本、奥地利专家担任编辑。ISO/IEC 4922-2 基于 ISO/IEC 19592-2 给出了秘密共享技术的安全多方计算机制。本文件中规定的机制包括加法、减法、常数乘法、共享随机数生成和乘法。
5.	ISO/IEC 11770-8	Information technology — Security techniques — Part 8: Password-based key derivation	信息技术 安全技术 第 8 部分：基于口令的密钥推导	NP	该项目由日本提出，日本、卢森堡、俄罗斯专家担任编辑。ISO/IEC 11770-8 规定了一种密钥推导函数，其将人们日常使用的口令作为密钥推导函数的输入，输出所需的加密密钥。本文件适用于需要从口令推导出加密密钥的应用场景。