

附件 2：10 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 27036-3	Cybersecurity — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security	网络安全 供应商关系 硬件、软件和服务供应链安全指南	DIS	该项目由美国专家担任编辑。ISO/IEC 27036-3 按照系统生命周期过程定义了各阶段供应链双方的安全指南，此次修订主要是将 ISO/IEC 27036-3 内 ICT 相关内容根据 ISO/IEC/IEEE 15288:2015 《系统和软件工程 系统生命周期管理》进行调整，使两个标准的语境一致，利于标准发布后的衔接应用。
2.	ISO/IEC 27006-2	Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems	信息技术 网络安全和隐私保护 信息安全管理体系审核与认证机构的要求 第 2 部分: 与 ISO/IEC 27701 相关的要求	CD	该项目由日本、美国和英国专家担任编辑。ISO/IEC 27006-2 在 ISO/IEC 27006:2021 基础上，从能力和认证过程两方面对隐私信息管理体系（PIMS）认证机构提出了补充要求，主要涉及审核员能力、审核时间计算、ISO/IEC 27701 认证与 ISO/IEC 27001 认证之间的关系等内容。

序号	标准编号	英文名称	中文名称	阶段	标准内容
3.	ISO/IEC 27553-2	Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 2: Part 2: remote modes	信息技术 安全技术 移动设备生物特征识别身份认证安全要求 第 2 部分: 远程模式	NP	该项目由中国、法国和日本专家担任编辑。ISO/IEC 27553-2 由我国主导提出的 ISO/IEC 27553 拆分而来。ISO/IEC 27553-2 主要包含使用移动设备生物特征识别能力进行用户身份认证的实现模式分析、安全威胁分析、安全要求的定义、以及隐私保护相关考虑等。本部分不涵盖生物特征数据不离开移动设备的场景, 即本地模式。
4.	ISO/IEC 6109	Cybersecurity — Guidelines for security monitoring of data life cycle processes	网络安全 数据生命周期过程安全监测指南	NP	该项目由中国专家提出。ISO/IEC 6109 提出了通过控制日志记录功能的有效性保护数据生命周期的指南, 可应用于数据生命周期日志管理、数据安全事件监测预警、分析追溯等。
5.	ISO/IEC 24760-4	IT Security and Privacy — A framework for identity management — Part 4: Part 4: Authenticators, Credentials and Authentication	信息安全与隐私 身份管理框架 第 4 部分: 身份验证器、凭据和身份验证	NP	该项目由德国和比利时专家担任编辑。ISO/IEC 24760-4 提供了实施认证和使用凭证的指南, 描述了用于实现具有不同操作的用户身份验证的互补模型, 提出了认证的方法。

序号	标准编号	英文名称	中文名称	阶段	标准内容
6.	ISO/IEC 27561	Information technology — Security techniques — Privacy operationalisation model and method for engineering (POMME)	信息技术 安全技术 工程隐私操作化模型及方法	CD	该项目由意大利、印度和法国专家担任编辑。ISO/IEC 27561 描述了一种将隐私原则实施为控制和功能的模型和方法，支持联网的、相互依赖的应用程序和系统，适用于开发系统控制或处理 PII 的工程师和其他从业人员。
7.	ISO/IEC 29128-3	Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 3: Part 3: Evaluation Methods and Activities for Protocol Implementation Verification	信息安全，网络安全和隐私保护 密码协议验证 第 3 部分：协议实现验证的评估方法和活动	NP	该项目由法国专家担任编辑。ISO/IEC 29128-3 定义了评估方法和活动，确保 ISO/IEC 15408-4 的框架评估加密协议实现的正确性，该标准主要包括：通过/失败标准的评估方法、实现保障级、保障组件、脆弱性评估和验证工具等。
8.	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 2 部分：密码协议的评估方法和活动	NP	该项目由法国专家担任编辑。ISO/IEC 29128-2 给出评估 ISO/IEC 29128-1 中所定义内容的评估方法和活动，确保 ISO/IEC 15408-4 的框架验证加密协议规范的正确性和安全性。该标准主要包括：评估自动化证明工具、评估协议模型、评估模型化结果等。

序号	标准编号	英文名称	中文名称	阶段	标准内容
9.	ISO/IEC 29192-8	Information security — Lightweight cryptography — Part 8: Authenticated encryption	信息安全 轻量级密码 第 8 部分: 鉴别加密	FDIS	该项目由瑞士专家担任编辑。ISO/IEC 29192-8 规定了一种适用于有轻量级加密机制需求的鉴别加密方法, 能够防止未经授权的数据泄露, 并使数据接收者能够验证所接收的数据是否被篡改, 用于实现数据完整性和机密性的安全目标。
10.	ISO/IEC 27563	Security and privacy in artificial intelligence use cases	隐私保护 人工智能用例 中的安全和隐私	CD	该项目由中国、瑞士、菲律宾、印度、德国和韩国专家担任编辑。ISO/IEC 27563 提供了有关如何评估人工智能用例中安全性和隐私性的内容, 并在安全和隐私问题、安全和隐私风险、安全和隐私控制、安全和隐私保证以及安全和隐私计划方面对相应的人工智能系统用例进行总体评估。