附件

《基于大模型的网络攻击行为建模与防御技术要求》等4项团体标准立项计划

项目计划号	标准名称	主要内容	计划完成时间	牵头单位
140-T/ISC-25	《基于大模型的网络攻击行为建模与防御技术要求》	本文件规定了基于大模型的网络攻击行为建模与防御的术语和定义、攻击行为建模技术要求、防御技术要求、安全评估和测试。 本文件适用于大模型在网络攻击检测、行为分析、威胁建模和防御措施中的应用，适用于大模型开发方、部署方、服务提供方和评估机构。	26.6	华兴中科标准技术(北京)有限公司
141-T/ISC-25	《智能防火墙检测与防御能力要求》	本文件规定了智能防火墙的防御能力要求、阻断能力要求和测试方法。 本文件适用于智能防火墙的设计、开发、测试和部署。	26.6	华兴中科标准技术(北京)有限公司

142-T/ISC-25	《互联网的关键领域AI训练数据可信质量要求》	本文件规定了关键领域AI训练数据在采集、预处理、标注、存储、传输、使用及处置等环节的可信质量要求。 本文件适用于关键领域AI系统的训练数据提供者、处理者及使用者开展数据质量管理活动，也可用于第三方评估机构进行数据质量评估。	26.6	华兴中科标准技术(北京)有限公司
143-T/ISC-25	《AI算法可解释性与决策透明度通用技术规范》	本文件规定了AI算法可解释性与决策透明度的术语和定义、技术要求、评估方法。 本文件适用于各类AI系统的开发、部署和和评估等全生命周期过程，为各类组织提供可解释性与透明度的技术指导。	26.6	中国联通国际有限公司