附件 1

2025 年度第一批网络安全国家标准需求清单

序号	标准名称	类型	主要内容	拟解决问题	工作组
1.	网络安全技术 汽车采集车外数据一键管控技术要求	制定	本标准针对智能网联汽车大量采集车外环境敏感数据的风险隐患，对智能网联汽车采集的车外数据提出安全管控要求。	智能网联汽车采集的车外数据缺乏安全管控方面的国家标准，本标准通过明确智能网联汽车采集的车外数据一键管控功能技术要求，旨在解决重要环境信息和个人隐私数据的保护问题。	WG2
2.	网络安全技术 移动通信信号屏蔽器技术要求	制定	本标准针对移动通信信号屏蔽需求，对移动通信信号屏蔽器的屏蔽方式、屏蔽频率范围、带宽、功率强度以及杂散发射等方面提出技术指标要求。	移动通信屏蔽器缺乏统一的国家标准，本标准通过明确移动通信信号屏蔽器各项技术指标，旨在指导移动通信信号屏蔽器的研制、生产，达到屏蔽效能精准有效、绿色环保的目标。	WG2

序号	标准名称	类型	主要内容	拟解决问题	工作组
3.	网络安全技术 密码设备应用接口规范	修订	本标准拟修订GB/T 36322—2018《信息安全技术 密码设备应用接口规范》，规定公钥密码基础设施应用技术体系下服务类密码设备应用接口的算法标识、数据结构和接口函数，拟增加多包对称加解密、多包MAC计算和单包可鉴别加解密、多包可鉴别加解密、带密钥的杂凑运算、SM9标识密码算法等相关接口函数及定义。	本标准拟解决目前SM9标识密码算法在推广应用过程中接口标准有待统一、密码应用安全性评估中缺少HMAC相关接口的问题。	WG3
4.	网络安全技术 密码模块安全要求	修订	本标准拟修订GB/T 37092—2018 《信息安全技术 密码模块安全要求》，规定密码模块安全等级和要求，拟更新细化软件密码模块安全要求、完善核准的安全功能列表、合理调整核准的身份鉴别机制等内容。	随着密码产品技术和形态创新，原标准难以覆盖且部分技术内容已滞后，造成依据本标准不能实施安全检测的问题，另外，本标准编制过程中参考的FIPS 140-2正在向FIPS 140-3迁移，标准有必要对相关内容重新进行技术修订。	WG3
5.	网络安全技术 物理不可克隆功能安全技术规范	制定	本标准拟规定物理不可克隆功能（PUF）的总体框架、接口、处理模块、应用、生命周期管理、安全要求以及测试评估方法。其中，安全要求规定了PUF在稳定性、随机性等六个方面的要求，测试评估方法包括对安全要求的测试方法。	拟解决硬件安全的脆弱性、物理设备唯一性标识认证、对抗硬件篡改的安全需求，作为保障物理设备唯一性标识认证和增强硬件安全的重要手段，国内缺乏PUF安全技术统一标准规范，明确不同类型PUF的应用场景和性能要求。	WG4

序号	标准名称	类型	主要内容	拟解决问题	工作组
6.	网络安全技术 基于多信道的证书申请和应用协议	修订	本标准拟修订GB/T 40018—2021《基于多信道的证书申请和应用协议》，修订证书申请相关部分，添加对国密双证书支持；修订URI编码格式，添加对自定义第三方TAG的支持；	拟解决原标准仅因仅使用单证书体制，无法对接现有的国密双证书系统，传统的URI编码方案不再满足多终端多应用在多场景下的扫码需求等问题，需要提升URI编码方案与现有移动端浏览器及其他应用程序的兼容能力。	WG4
7.	网络安全技术 消费类智能联网设备安全要求	制定	本标准拟规定消费类智能联网设备标识鉴别、访问控制、硬件和软件安全、口令保护、数据和个人信息安全等安全技术和安全保障要求。	解决当前联网摄像头、家用路由器、智能穿戴设备等消费类智能联网设备自身安全防护能力薄弱，缺乏统一的安全规范要求，为推动相关产品安全能力提升、打通国际国内产业互认提供技术依据。	WG5
8.	网络安全技术 工业控制系统安全管理基本要求	修订	本标准拟修订GB/T36323-2018,规定工业控制系统网络安全管理模型及该模型包含的主要内容，并提出资产管理、配置管理、安全评估、供应链安全、意识培训等工业控制系统网络安全管理和安全运营各级措施。	拟解决当前标准内容已不能完全适用当前新技术应用发展形势，缺乏对工业互联网安全、云平台安全、商用密码应用安全等新相关风险和内容的考虑。	WG5
9.	网络安全技术 网络安全等级保护定级指南	修订	本标准结合大量定级实践经验和监管需求，修订等级划分依据，规定定级对象选取的原则与方法，梳理定级对象的类型，并根据使用的不同新技术总结定级对象	随着数字经济的快速发展，企业的业务模式不断创新，业务方向也更加多元化、差异化。人工智能、边缘计算等新技术的不断应用、具有行业特点的安全需求不断提	WG5

序号	标准名称	类型	主要内容	拟解决问题	工作组
			的基本特征；新增定级对象边界确定方法，避免遗漏关键资产。	出都给网络安全等级保护定级工作带来了新的挑战。	
10.	网络安全技术 网络安全漏洞分类分级指南	修订	本标准给出网络安全漏洞的分类方式、分级指标及分级方法指南。修订内容主要包括增加分类角度，丰富漏洞类别，优化分级方法，以适应产品提供者、网络运营者、漏洞收录组织、漏洞应急组织等不同使用者，在落实国家漏洞管理新政策和满足漏洞管理技术新需求时的新需要。	拟解决当前标准内容漏洞类别覆盖不全、漏洞级别划分无法应对威胁场景动态变化等问题，细化分级因素中的“环境因素”，并在漏洞分级方法“环境因素评级”中更加强调漏洞随时间和环境变化带来的危害变化。	WG5
11.	网络安全技术 网络安全漏洞标识与描述规范	修订	本标准拟修订GB/T 28458—2020《网络安全漏洞标识与描述规范》，补充受网络安全漏洞影响产品的描述方式，通过规范的字符串表述方法对信息产品版本进行枚举表述，建立漏洞与受该漏洞影响具体版本间的关联关系。	拟规范受漏洞影响产品描述形式，规范产品厂商自身产品版本管理和漏洞批露行为，整合厂商、安服企业、用户等多方力量汇聚我国信息类产品使用领域、特点、行业等信息。	WG5
12.	网络安全技术 集成电路芯片通用安全规范	制定	本标准拟围绕集成电路芯片生命周期各环节提出芯片安全框架，明确芯片安全分级要求和对应安全检测方法，给出示范案例或环境条件说明。	拟解决现有集成电路芯片安全强度不足、安全能力不统一、检测标准缺失的问题，防范芯片被解剖、被探测、被复制、被攻击等风险，提升芯片安全韧性和不用应用环境下的安全级别可选择性。	WG5

序号	标准名称	类型	主要内容	拟解决问题	工作组
13.	网络安全技术 卫星互联网网络安全框架	制定	本标准拟提出卫星互联网网络安全技术框架和接入安全要求，指导卫星互联网分域安全设计、开发和应用，为卫星互联网安全参与相关方、运维者和用户提供指南。	当前卫星互联网网络接入和数据安全风险突出，拟解决相关网络安全要求不明晰、标准缺乏的问题，能够指导卫星互联网安全基础技术研发和安全产业生态体系建设等。	WG6
14.	网络安全技术 信息安全风险评估实施指南	修订	本标准拟修订GB/T 31509—2015《信息安全风险评估实施指南》，提出网络安全风险评估实施各阶段的具体操作指南，包括要素关系、分析原理、实施流程、评估内容以及各阶段的实施要点和工作方法等。	近年来，网络安全法律法规和GB/T 20984-2022《信息安全技术 信息安全风险评估方法》对评估提出最新要求，拟解决现有标准内容与最新要求不一致的问题。适用于各类安全评估机构或被评估组织对信息系统网络安全风险评估项目的管理，指导风险评估项目的组织、实施、验收等工作。	WG7
15.	网络安全技术 信息安全治理	修订	本标准拟修订GB/T 32923-2016《信息技术 安全技术 信息安全治理》，在新版GB/T 22080的基础上，对信息安全管理体系各环节中治理相关活动的要求进行细化和阐释，更新了信息安全治理的目标和过程。	本标准可为组织明确信息安全治理的概念、目标和过程提供指导，组织可以通过这些指导来评估、指导、监控和沟通组织内与信息安全相关的过程。	WG7

序号	标准名称	类型	主要内容	拟解决问题	工作组
16.	网络安全技术 网络安全威胁信息质量评价指标和方法	制定	本标准拟提出网络安全威胁信息质量评价的基本原则、评价指标及评价方法。适用于指导各类组织和个人在网络安全威胁信息共享与质量评价等活动。	拟解决目前缺乏对威胁信息质量的评估机制，大量的低信息含量、无效的威胁信息对分析和研判网络安全态势和预警响应工作造成了严重的影响，限制了威胁信息流动和共享的实际效能等问题，建立一套科学合理的网络安全威胁信息质量评价体系。	WG7
17.	网络安全技术 网络安全事件管理 第4部分：协同	制定	本标准拟等同采用ISO/IEC 27035-4，提出多组织间以协同方式处理网络安全事件的指南。本文件还指出了外部合作对单个组织内部事件管理的影响，并为单个组织协调的事件管理过程提供指南。	拟解决跨组织边界的网络安全事件发生时，各相关方如何协同合作共同完成网络安全事件处置、以尽可能降低跨组织网络安全事件对组织的影响。	WG7
18.	数据安全技术 网络数据爬取行为规范	制定	本标准拟提出使用自动化工具收集网络数据的安全原则，规定使用自动化工具收集网络数据的总体要求、自动化工具技术要求和使用要求、自动化工具收集行为影响评估要求、已收集数据处理要求和网络数据披露方行为准则。	拟支撑《网络数据安全管理条例》第十八条关于自动化工具收集数据的要求，拟解决因大规模、高频率地爬取数据，影响正常用户的访问体验，甚至可能窃取用户的隐私信息或者商业机密等敏感数据等问题。	WG8

序号	标准名称	类型	主要内容	拟解决问题	工作组
19.	数据安全技术 小型个人信息处理者个人信息保护指南	制定	本标准拟明确小型个人信息处理者的界定因素，提出小型个人信息处理者在处理个人信息时的安全保护原则和安全措施等。	拟支撑《个人信息保护法》第六十二条关于针对小型个人信息处理者制定专门的个人信息保护规则、标准的要求，规范小型个人信息处理者合理合法处理个人信息活动。	WG8
20.	数据安全技术 数据提供、委托处理、共同处理安全指南	制定	本标准拟提出数据对外提供、委托处理、共同处理安全指南，明确安全举措、评估指南等内容。	拟支撑《网络数据安全管理条例》第十二条、第三十一条关于提供个人信息和重要数据提供、委托处理、共同处理安全要求。	WG8
21.	数据安全技术 个人信息保护合规审计服务能力要求	制定	本标准拟明确提供个人信息保护合规审计服务的机构和人员的管理能力、技术能力等相关要求。	拟支撑《个人信息保护法》第六十四条规定由专业机构开展的个人信息保护合规审计工作，解决个人信息保护合规审计专业机构能力难认定的问题。	WG8

序号	标准名称	类型	主要内容	拟解决问题	工作组
22.	数据安全技术 个人信息安全规范	修订	本标准拟修订GB/T 35273-2020《信息安全技术 个人信息安全规范》，根据《个人信息保护法》等法律法规最新要求，吸纳主管监管部门开展个人信息保护工作中的相关经验，与现行法律法规配套衔接。	拟支撑《个人信息保护法》《网络数据安全管理条例》《个人信息保护合规审计办法》等法律法规落地实施，提升标准在个人信息保护工作中的指导性和实用性，为个人信息安全提供更全面的保障。	WG8
23.	数据安全技术 数据安全产品分类指南	制定	本标准拟规定数据安全产品分类，包括数据安全管理类、数据安全技术类、数据安全合规类及其他类四个方面。本文件适用于数据安全产品企业参照明确产品分类，同时也为数据处理者开展数据安全防护能力建设时选取数据安全产品提供参考。	拟通过调研我国工业和信息化领域数据安全产品技术及产业发展现状，研制工业和信息化领域数据安全产品分类指南，摸清数据安全产品市场类型底数，明确细分领域产品技术指标基线，为主管部门数据安全产品产业治理提供标准化抓手，为数据安全产品应用企业提供标准化参考依据。	WG8

序号	标准名称	类型	主要内容	拟解决问题	工作组
24.	数据安全技术 数据安全从业人员能力建设指南	制定	本标准拟提出数据安全从业人员能力培养目标、技术知识和技能条件、考核评估方法等，同时给出适宜的人员培训方法、培训教材编写、培训机构与师资配置及管理流程等指南。	旨在解决我国数据安全领域面临的三大挑战:人才数量短缺、从业人员质量参差不齐、以及缺乏人才评价和认证体系。此外，从业人员在技术基础、持续进步潜力、法律法规理解、治理和风险评估方面的能力参差不齐，难以满足日益增长的数据安全要求。	WG8
25.	数据安全技术 数据安全能力成熟度模型	修订	本标准拟提出组织机构数据安全保障的能力成熟度模型，以数据为中心，重点围绕数据处理活动，从组织建设、制度流程、技术工具和人员能力四个方面进行安全保障。适用于对组织机构数据安全能力进行评估，也可供组织机构开展数据安全能力建设时参考。	拟解决现行GB/T 37988—2019《信息安全技术 数据安全能力成熟度模型》与数据安全法提出的数据处理活动划分思路不一致等问题。	WG8
26.	网络安全技术 人工智能安全能力成熟度评估方法	制定	本标准拟给出人工智能安全能力的成熟度模型架构，明确安全能力要素、能力成熟度等级、人工智能安全过程等维度，规定人工智能系统设计、研发、训练、测试、部署、使用、维护等生命周期各环节的安全能力成熟度等级要求以及评估方法。	人工智能应用日益广泛，但人工智能技术及应用过程中产生的各类安全问题极易对社会生产生活产生负面影响。当前缺乏对人工智能安全能力成熟度的统一模型架构与评估方法，难以应对不同抗风险能力使用场景对人工智能安全能力的不同安全需求。	SWG-ETS

序号	标准名称	类型	主要内容	拟解决问题	工作组
27.	网络安全技术 人工智能应用安全分类分级方法	制定	本标准拟从安全角度给出人工智能应用的分类分级方法，提出人工智能应用安全分类分级的基本原则、框架、流程，以及分类方法、分级方法等，并给出人工智能应用安全分类分级参考示例。	人工智能应用场景多样，安全风险以及安全需求差异较大，目前缺乏统一的安全分类分级标准。高风险场景（如医疗诊断或自动驾驶）安全保障不足可能导致严重后果，低风险场景（如智能翻译）则可能面临资源浪费，人工智能应用安全管理缺乏系统性。	SWG-ETS
28.	网络安全技术 人工智能技术涉及未成年人应用安全指南	制定	本标准拟规定将人工智能技术应用在涉及未成年人的网络应用中的总体原则、关键参与角色、生命周期关键阶段安全要求、网络环境净化、不公平风险防范、问责和补救措施等方面的安全指南。	人工智能技术广泛应用于涉及未成年人的网络产品和服务中,拟解决存在的AI滥用导致内容安全与心理健康、算法偏见与歧视、教育与认知发展以及法律伦理、不正当经济消费行为等问题。	SWG-ETS

序号	标准名称	类型	主要内容	拟解决问题	工作组
29.	网络安全技术 云计算服务安全责任划分指南	制定	本标准拟提出在不同的云能力类型下，云服务提供者、硬件服务提供者、软件服务提供者、运维服务提供者、安全服务提供者以及云用户的网络安全责任划分的参考原则及实施方法。	拟解决目前云计算行业中多角色安全责任划分不清晰、核心云服务能力层层外包导致安全管理责任落空，缺乏对各参与方角色安全责任划分及技术控制的指导等问题。适用于云服务参与方开展云计算服务的规划、建设、运营的活动。也可为评估机构开展多方角色参与情况下的云服务安全评估提供参考依据。	SWG-ETS
30.	网络安全技术 区块链系统安全实施指南	制定	本标准拟规定区块链系统安全实施的操作指南，包括区块链系统设计、开发、部署、运行和维护等阶段，给出实施运行的安全操作规范。	拟针对区块链系统实现和应用过程中面临的诸多安全风险，从网络层、共识层、合约层等各维度给出系统级安全实施指南，规范区块链系统设计、开发、部署、运行和维护，也为区块链信息服务提供者、第三方评估机构和相关主管部门提供参考。	SWG-ETS