附件 1

2024 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 SM9 密码算法加密签名消息格式	制定	本标准拟规定 SM9 密码算法的加密和签名消息语法。适用于使用 SM9 算法进行加密和签名操作时对数据结果的标准化封装。	本标准拟解决 SM9 密码算法在数字签名、加解密和密钥协商等密码应用中的签名结果、密文结构和密钥协商数据结构语法的标准化定义问题，以使 SM9 密码算法的各密码产品能互通互认。	WG3
2	网络安全技术 二元序列随机性检测方法	修订	本标准拟修订 GB/T 32915-2016《信息安全技术 二元序列随机性检测方法》，拟规定商用密码应用中二元序列随机性检测的检测指标和检测方法。修订内容包括修改游程分布检测中的统计值构造方法，增加和修改检测模式、计算方法等。	本标准可用于检测二元序列样本是否具有良好的随机统计特性，可为各类随机数发生器的设计、研制、检测等提供指导。	WG3
3	网络安全技术 密码应用标识	修订	本标准拟修订 GB/T 33560-2017《信息安全技术 密码应用标识规范》，修订内容包括调整补充相关密码算法、数据格式、协议标识以及及商用密码领域中相关 OID 定义。	本标准拟解决标识定义不统一的问题，通过规范密码协议接口、管理等各方面使用的标识，实现密码基础设施各组件间的兼容和统一，指导密码设备研制和协议开发，有利于管理部门实施有效的管理。	WG3
4	网络安全技术 SM2 密码算法加密签名消息格式	修订	本标准拟修订 GB/T 35275-2017《信息安全技术 SM2 密码算法加密签名消息语法规范》，修订内容包括增加签名数据类型、数字信封类型、加密数据类型、密钥协商类型等示例；完善对不安全的定义、类型；	本标准通过规范 SM2 密码算法进行加密和签名操作时对相关数据的标准化封装，解决受不同领域软硬件及信息系统开发商在处理密码数据时可能遇到的格式不兼容的问题。从而提升不同系统或不同模块间的互联互通，提升对	WG3

序号	标准名称	类型	主要内容	拟解决问题	工作组
			删除涉及属性证书的描述。	接效率，保障通信协议安全性。	
5	网络安全技术数控系统商用密码应用技术要求	制定	本标准拟规定数控系统商用密码应用的技术要求，包括商用密码应用的总体要求、密码应用技术框架、对应不同安全级别的具体密码应用技术要求等。	本标准拟指导智能制造及相关领域企业进行数控系统的设计开发、生产制造、应用场景等多个方面安全防护要求，保障数控系统稳定、高效、安全运行，推动密码技术在数控系统中标准化应用推广，提高数控系统的整体安全防护水平。	WG3
6	网络安全技术秘密分享技术框架	制定	本标准拟修改采用 ISO/IEC 19592《Information technology — Security techniques — Secret sharing》，提出秘密分享方案的一般模型、功能和性质，规范几类典型的实现方法，适用于指导秘密分享技术的设计与使用。	本标准拟解决数据的安全拆分和恢复问题，为当前隐私计算、机器学习、区块链等前沿技术应用中的敏感数据存储、隐私数据拆分提供可证明安全的密码学工具，从而加强数据安全保护。	WG3
7	网络安全技术开放的第三方资源授权协议框架	制定	本标准拟规定第三方资源授权协议的流程、不同类型的授权许可、协议各端点的功能要求以及系统实体之间传递消息的格式和参数要求等。	本标准拟解决互联网中跨安全域的资源共享问题，实现用户可利用某个安全域中的应用程序访问另一个安全域中受保护的资源，满足日益增长的大量网络应用频繁交互与资源共享需求。	WG4
8	网络安全技术零信任成熟度模型	制定	本标准拟提出实现零信任能力应具备的身份安全、基础设施、网络安全、数据安全、应用和负载安全、网络可持续安全检测与评估、网络安全可视化等方面的要求，并划分阶段形成零信任能力成熟度评定方法。	本标准针对零信任能力建设及评价缺乏统一的标准依据问题，拟明确零信任各关键能力特征的技术要求，规范零信任相关生产开发者的功能设计与产品运营实践机制。	WG4

序号	标准名称	类型	主要内容	拟解决问题	工作组
9	网络安全技术 鉴别与授权 基于属性的访问控制模型	制定	本标准拟给出基于属性的访问控制（ABAC）概念、参考模型组成、工作机制及基于属性的访问控制策略实现等内容。	本标准拟解决传统的静态访问控制难以满足的，针对适用于大型企业的动态、持续和细粒度的访问控制要求的问题。	WG4
10	网络安全技术 引入可信第三方的实体鉴别及接入架构规范	修订	本标准拟修订 GB/T 28455-2012《信息安全技术 引入可信第三方的实体鉴别及接入架构规范》，规定引入可信第三方的实体鉴别及接入架构的一般方法，新增原子密钥建立与实体鉴别机制等内容。	本标准拟解决终端和网络通信前，通过鉴别和授权功能互相鉴别对方身份的合法性，以保证通信的安全问题。	WG4
11	网络安全技术 网络安全产品互联互通 第 4 部分 功能接口	制定	本标准拟提出支撑不同网络安全产品互联互通的接口协议、请求方式和安全机制，适用于指导网络安全产品的设计、开发、应用和测试。	本标准拟解决当前网络安全产品功能接口实现方式不一致、接口描述内容不统一等带来的网络安全信息难以高效整合利用、安全功能难以有效协同的问题。	WG5
12	网络安全技术 网络安全产品互联互通 第 5 部分 行为信息格式	制定	本标准拟提出支撑不同网络安全产品互联互通的行为信息格式、字段和内容描述。适用于网络安全产品的设计、开发、应用和测试。	本标准拟解决当前网络安全产品行为信息由于格式不统一带来的信息内容难以有效整合利用、信息传递效率低等问题。	WG5
13	网络安全技术 网络安全产品互联互通 第 6 部分：威胁信息格式	修订	本标准拟修订 GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》，优化和细化网络安全威胁信息模型，补充完善网络安全威胁信息中各组件的属性和属性值格式等信息。	本标准拟支撑我国信息共享制度的建设，解决网络安全产品及各组织信息共享过程中威胁信息格式不一致，难以信息共享等问题。	WG5
14	网络安全技术 电子邮件系统安	修订	本标准拟修订 GB/T 37002-2018《信息安全技术 电子邮件系统安全技术要求》，	本标准拟解决电子邮件系统面临的钓鱼邮件、内容泄密和身份仿冒等问题。	WG5

序号	标准名称	类型	主要内容	拟解决问题	工作组
	全技术规范		规定电子邮件系统安全要求和测试评价方法。修订内容包括新增防钓鱼邮件方面的安全机制，补充对应的测试评价方法等内容。		
15	网络安全技术移动智能终端未成年人模式联动要求	制定	本标准主要对标《移动互联网未成年人模式建设指南》，细化智能终端、APP 和应用商店实现三方联动应当具备的技术和功能标准。	本标准拟解决未成年人模式建设过程中涉及的软硬件联动技术接口、功能实现技术方案等问题。	WG5
16	网络安全技术未成年人产品和服务网络保护要求	制定	本标准拟规定未成年人产品和服务在个人信息和网络权益等方面的保护要求，提出移动互联网应用程序（App）、未成年人网络保护软件、专门供未成年人使用的智能终端等安全措施。	本标准拟规范未成年人产品服务提供者在开发运营过程中强化未成年人个人信息保护与网络权益保护机制。	WG5
17	网络安全技术网络存储安全技术要求	修订	本标准拟修订 GB/T 37939-2019《信息安全技术 网络存储安全技术要求》，规定存储设备安全能力分级要求，修订内容包括从系统安全、数据安全、安全管理等维度提出不同层级的存储安全能力要求。	本标准拟落实《数据安全法》、《工业和信息化领域数据安全管理办法(试行)》，聚焦数据如何分类分级重点，解决当存储设备所承载的数据等级不同时，对应的存储设备也应提供相应安全能力，从而保障所存储数据的安全性等问题。	WG5
18	网络安全技术嵌入式操作系统安全规范	制定	本标准拟提出嵌入式操作系统的通用安全技术要求和测评方法，适用于指导嵌入式操作系统的设计、开发和测试。	本标准拟落实《网络安全法》《数据安全法》对应用系统相关安全性要求，解决当前嵌入式操作系统安全依旧存在技术实施不规范的问题，缺乏统一的安全评价体系，进一步规范嵌入式操作系统安全性检查手段。	WG5

序号	标准名称	类型	主要内容	拟解决问题	工作组
19	网络安全技术 计算机 BIOS 安全技术规范	制定	本标准拟规定计算机 BIOS 系统的访问控制、身份鉴别、完整性度量、系统安装来源验证、可信恢复、安全升级等安全功能的基础要求和增强要求。	本标准拟针对关键信息基础设施应用的计算机设备的 BIOS 自身安全防护薄弱、供应链种类繁多，缺乏统一的要求标准问题，规范计算机 BIOS 操作系统安全功能模块的设计、开发和使用，从而提升计算机 BIOS 系统及应用的安全防护水平。	WG5
20	网络安全技术 网络安全等级保护测评机构能力要求和评 估规范	修订	本标准拟修订 GB/T 36959-2018《信息安全技术 网络安全等级保护测评机构能力要求和评估规范》，修订内容包括调整补充“组织管理能力”、“测评实施能力”、“设施和设备安全与保障能力”、“质量管理能力”、“规范性保证能力”等方面内容。	本标准拟解决现行标准与最新测评机构管理政策、已修订的等级保护技术标准不一致的问题，同时按照标准实践经验，细化完善部分标准条款。	WG5
21	网络安全技术 操作系统安全技术规范	修订	本标准拟合并修订 GB/T 20272-2019《信息安全技术 操作系统安全技术要求》和 GB/T 20008-2005《信息安全技术 操作系统安全评估准则》，规定操作系统的安全技术要求和测试评价方法。修订内容包括调整补充密码支持、数据分类分级、访问控制等相关要求和测试评价方法。	本标准作为 GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》配套标准，确保该类产品作为网络、信息系统中最基础的组件，适应当前数据安全、密码技术等最新要求，具备应有的安全功能和自身安全保护能力。	WG5
22	网络安全技术 量子密钥分发的安全要求、测试和评估方法 第 1 部分：要求	制定	本标准拟等同采用国际标准 ISO/IEC 23837-1:2023，明确各种量子密钥分发（QKD）协议和实现的一般框架模型，提出该模型下 QKD 需满足的通用安全功能要求集，适用于对离散（DV）和连续（CV）编码，以及准备-测量（PM）、设备无关	本标准拟解决 QKD 产品缺乏统一的安全性设计要求，分析不同 QKD 协议面临的安全威胁、环境假设和实现缺陷，特别是分析量子光学部件相关的侧信道安全等问题需要满足的安全功能要求，为 QKD 相关技术产业的安全和规范性发展提供指导。	WG5

序号	标准名称	类型	主要内容	拟解决问题	工作组
			（MDI）及基于纠缠（EB）的 QKD 模块的安全测评工作。		
23	网络安全技术 量子密钥分发的安全要求、测试和评估方法 第2部分：测试和评估方法	制定	本标准拟等同采用国际标准 ISO/IEC 23837-2:2023，规定量子密钥分发（QKD）技术的安全测评方法，覆盖 QKD 协议、发送模块、接收模块，以及校准过程的安全测试和评估方法，特别是 QKD 技术的脆弱性分析和攻击潜力计算方法，适用于所有类型的 QKD 产品。	本标准拟解决 QKD 协议和量子光学部件安全测评中面临的协议实现的符合性、发送端和接收端抵抗已知光学侧信道攻击的强度，以及攻击复杂性的计算及与安全级别的对应性等问题，为 QKD 产品分级安全测评提供依据。	WG5
24	网络安全技术 具有中央处理器的 IC 卡芯片安全规范	修订	本标准拟修订 GB/T 22186-2016《信息安全技术 具有中央处理器的IC卡芯片安全技术要求》，修订内容包括更新 IC 卡芯片的安全功能要求和安全保障要求，增加测试和评估方法等。	本标准拟解决当前标准不适于依据最新版的 GB/T 18336 标准开展测评的问题，以指导对 IC 芯片的脆弱性分析和穿透性测试。	WG5
25	网络安全技术 软件安全开发能力成熟度模型	制定	本标准拟给出安全开发的标准定义，对安全开发活动的公共特征进行五级描述，构建安全开发能力评估模型。适用于组织机构自身软件安全开发能力评估和过程改进，也适用第三方开展能力评估。	本标准拟以工程化的方法解决现代软件开发面临在复杂环境下群体开发活动导致的软件代码质量和安全隐患的问题，通过标准化的能力级别划分，解决安全开发过程的分级评估操作办法。	WG5
26	网络安全技术 信息系统安全保障评估框架 第2部分： 安全保障要求	修订	本标准拟修订 GB/T 20274.2、GB/T 20274.3 和 GB/T 20274.4。修订内容包括将技术保障、管理保障和工程保障的要求合并，补充供应链、数据安全、网络反间谍等方面等要求，重新定义能力成熟度等级划分等。	本标准拟应用能力成熟度模型和通用评估准则（CC）的思路对网络安全保障体系（技术、管理和工程方面）开展能力等级评价工作。	WG5

序号	标准名称	类型	主要内容	拟解决问题	工作组
27	网络安全技术分布式控制系统（DCS）安全技术要求	制定	本标准拟规定分布式控制系统（DCS）的安全功能要求和安全保障要求，包括设备标识安全、漏洞和恶意程序防范、访问控制安全、日志审计安全、通信安全、数据安全等内容。	本标准拟针对广泛应用的分布式控制系统（DCS）面临的网络安全风险问题，为DCS产品设计、开发、部署和测评提供重要依据。	WG5
28	网络安全技术网络空间可视化表达方法	制定	本标准拟提出网络空间可视化表达的原则、层次、内容和方法，规定地理环境、网络环境、行为主体和业务环境数据的表达方式，对网络空间要素、关系和事件可视化。	本标准拟解决网络空间可视化框架和功能不统一的问题，适用于网络安全综合防控体系建设、网络安全挂图作战等工作。	WG5
29	网络安全技术网络空间测绘数据交换格式	制定	本标准拟规范资产测绘时的资产分类、数据格式，以统一来自不同资产测绘源的测绘数据。	本标准拟解决资产测绘时不同测绘源数据格式不统一问题，并为资产测绘数据共享、网络空间安全图谱构建提供基础数据。	WG5
30	网络安全技术工业控制系统网络安全防护能力成熟度模型	修订	本标准拟修订GB/T 41400-2022《信息安全技术 工业控制系统信息安全防护能力成熟度模型》，细化安全管理和安全运营，新增工业云平台、重要工业数据出境、建设网络安全运营中心等相关内容要求。	本标准拟解决当前我国工业控制系统综合安全防护能力缺乏科学评价方法、标准要求条款与新版政策文件要求不匹配的问题。通过本次修订，参照新版工业控制系统网络安全防护指南有关要求，对标准内容进行相应调整，可有效提升标准对主管部门政策落地支撑的契合程度。	WG5
31	网络安全技术物联网感知终端应用安全技术要求	修订	本标准拟修订GB/T 36951-2018《信息安全技术 物联网感知终端应用安全技术要求》，修订内容包括新增安全监测与运维管理等内容、更新数据安全与隐私保护相关要求等。	本标准拟解决物联网感知终端面临的仿冒、篡改、抵赖、信息泄露、Dos和提权等各种安全威胁，适用于物联网信息系统建设运维单位对感知终端进行安全选型、部署、运行和维护，也适用于指导感知终端设计和生产和开展安	WG6

序号	标准名称	类型	主要内容	拟解决问题	工作组
				全测试。	
32	网络安全技术物联网安全参考模型及通用要求	修订	本标准拟修订 GB/T 37044-2018《信息安全技术 物联网安全参考模型及通用要求》，修订内容包括更新物联网安全体系架构，新增数据安全、密码应用等要求。	本标准拟解决新技术新应用场景下，物联网技术演变与融合发展模式变化引发新的网络和数据安全风险问题。	WG6
33	网络安全技术移动终端安全技术规范	修订	本标准拟修订 GB/T 35278-2017《信息安全技术 移动终端安全保护技术要求》，修订内容包括基于新版 GB/T 35278 更新和增加安全功能组件、数据安全和安全等级要求、模块化评估方法等。	本标准拟解决当前版本标准技术内容缺少移动终端安全能力评估方法与评估等级等相关内容的问题，适用于移动终端的设计、开发、测试和采购。	WG6
34	网络安全技术关键信息基础设施安全监测预警实施指南	制定	本标准拟从安全技术、安全管理、安全保障等方面，提出关键信息基础设施运营者开展安全监测预警的措施和过程、方法。	本标准拟指导关基运营者规范开展关键信息基础设施安全监测预警，提升关键信息基础设施的安全能力，为国家关键信息基础设施安全保护、国家重大活动网络安全保障等重点工作提供技术支撑。	WG7
35	网络安全技术关键信息基础设施安全主动防御实施指南	制定	本标准拟作为 GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》的配套标准，提出实现关键信息基础设施主动防御相关要求的措施。	本标准拟指导关基运营者落实 GB/T 39204-2022 中主动防御的相关要求，提升关键信息基础设施的主动防御能力。	WG7
36	网络安全技术存储安全指南	制定	本标准拟修改采用 ISO/IEC 27040 国际标准，针对网络存储安全提出相应的安全管理措施和实施指南。	本标准拟指导存储基础设施的运营者和提供者在对系统进行安全规划时，对存储系统所面临的安全风险进行分析，并采用适当的安全控制措施以缓解这些风险。	WG7
37	网络安全技术网络安全事件调	制定	本标准拟等同采用 ISO/IEC 27043:2015，提出涉及数字证据的各种事件调查场景	本标准拟为众多网络安全事件调查过程提供指导方针，以确保在获得每个特定过程的结果	WG7

序号	标准名称	类型	主要内容	拟解决问题	工作组
	查 第1部分：事件调查原则和过程		中的共同事件调查过程，包括事前准备到调查结束的各个环节，以及对这些过程的任何一般性建议和注意事项。	时具有明确性和透明度。	
38	网络安全技术 网络安全事件管理 第1部分：事件管理原理	修订	本标准拟修订GB/T 20985.1-2017《信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理》，提出网络安全事件管理的基本概念、原理和过程以及关键活动。	本标准有助于组织理解网络安全事件管理的基本概念和原理，提出了一种结构化的网络安全事件管理过程方法，从而能够有准备且有序地开展网络安全事件管理活动。	WG7
39	网络安全技术 网络安全事件管理 第2部分：事件响应规划和准备指南	修订	本标准拟修订GB/T 20985.2-2020《信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南》，为GB/T 20985.1提出的网络安全事件管理过程中“规划和准备”和“经验总结”阶段提供实施指南。	本标准旨在通过提供网络安全事件响应的规划和准备以及从事件响应中吸取教训的详尽的指南，指导组织更好地开展网络安全事件管理各项活动。	WG7
40	网络安全技术 信息安全管理体系审核和认证机构要求	修订	本标准拟修订GB/T 25067-2020《信息技术 安全技术 信息安全管理体系审核和认证机构要求》，在GB/T 27021.1《管理体系审核认证机构 要求》的基础上，从认证机构的通用要求、结构要求、资源要求、信息要求、过程要求和管理体系要求六个方面，提出ISMS认证机构的特定要求和指南。	本标准修订拟与信息安全管理体系标准协调一致，解决ISMS认证审核中远程审核技术的应用、无固定场所的虚拟组织的认证、多场所审核时间计算、在ISMS认证证书中引用其他标准等问题。	WG7
41	网络安全技术 信息安全管理体系审核指南	修订	本标准拟修订GB/T 28450-2020《信息技术 安全技术 信息安全管理体系审核指南》，为信息安全管理体系审核方案管理	本标准拟解决与信息安全管理体系标准协调一致的问题，同时解决原标准扩展内容与GB/T 19011内容的重复性以及表述的准确性	WG7

序号	标准名称	类型	主要内容	拟解决问题	工作组
			和审核实施提供了指南，并对ISMS审核员能力提供评价指南。	等问题。	
42	数据安全技术云计算服务数据安全要求	制定	本标准拟针对云服务商运营管理、云服务客户采购使用云计算服务提出数据安全要求，给出云计算服务数据安全合同模板等。	本标准拟解决数据安全责任边界划分不清、重要数据和个人信息未进行专门保护、数据传输存储等关键环节未加密、未经同意处理云平台数据等云计算数据安全典型问题。	WG8
43	数据安全技术小型个人信息处理者个人信息保护要求	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要求等。	本标准拟支撑《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
44	数据安全技术会计审计服务数据安全要求	制定	本标准拟针对会计审计服务，围绕数据分级保护、数据跨境事项、数据处理安全等方面提出相关要求。	本标准拟支撑《会计师事务所数据安全管理暂行办法》的落地实施，解决会计审计服务过程中敏感数据泄露、数据违规跨境等问题。	WG8
45	数据安全技术匿名化处理指南	制定	本标准拟提供匿名化处理的实施指南。本文件适用于个人信息匿名化处理工作，也适用于开展个人信息安全管理、监管和评估。	本标准拟解决由于缺少统一的匿名化处理流程、匿名化程度判定规则、攻击测试方法等标准规范，导致匿名化工作不易落地的问题。	WG8
46	数据安全技术隐私计算通用框架	制定	本标准拟规定隐私计算通用框架，描述了参与角色、框架核心组件、基础功能，提供了隐私计算服务的实现机制。	本标准拟解决隐私计算兼容性差、生态隔离问题，降低跨平台迁移及互联互通障碍。	WG8
47	网络安全技术生成式人工智能内容标识方法	制定	本标准拟提出内容制作方利用人工智能技术生成或编辑文本、图片、音频、视频等内容，或利用人工智能技术生成沉浸式拟真场景时进行标识写入的方法，以及内容传播方对拟发布的人工智能生成内容	本标准拟解决人工智能生成内容的误用风险以及误导性内容的传播风险，通过显式标识提示用户当前内容由人工智能生成，避免用户误用生成内容，并通过隐式标识对生成内容来源进行确认，降低误导性生成内容的传播风险。	SWG-ETS

序号	标准名称	类型	主要内容	拟解决问题	工作组
			进行标识识别、验证、更新、展示的方法。		
48	网络安全技术人工智能代码生成服务安全要求	制定	本标准拟针对利用生成式人工智能技术所构建的代码助手类互联网信息服务，提出文书签署、代码审查、过程披露、风险提示等方面安全要求。	本标准拟解决人工智能生成代码质量参差不齐，存在输出漏洞代码、泄露用户数据等问题，指导相关组织机构开展自评估，提升代码助手类互联网信息服务和应用安全水平。	SWG-ETS
49	网络安全技术政务云安全配置基线要求	制定	本标准拟基于网络安全等级保护、云计算服务安全评估等要求，针对政务云平台的关键核心组件，包括虚拟机、容器、操作系统、云管平台、第三方组件等，提出安全配置基线要求。	本标准拟解决各级政务云平台缺乏统一安全配置标准，安全保护水平参差不齐问题，强化关键核心组件安全配置管理，提升我国政务云安全基准，降低云上业务安全风险。	SWG-ETS
50	网络安全技术政务云平台安全监测方法	制定	本标准拟提出政务云平台安全监测参考模型，以及云资源监测、安全运营监测、安全合规监测、安全事件监测等方面的技术指标。	本标准拟针对政务云平台安全风险动态变化、云平台架构弹性伸缩等特点，解决仅通过定期的静态云安全评估、等保测评等方法，难以保障相关安全措施持续有效，缺乏持续的动态监督措施等问题。	SWG-ETS