附件 1

2023 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
1	信息安全技术 生成式人工智能预训练和优化训练数据安全规范	制定	本标准拟针对生成式人工智能产品预训练和优化训练数据来源合法性，符合法律法规要求，不含侵犯知识产权内容，保护个人信息，保证真实性、准确性、客观性、多样性等方面提出安全规范。	本标准是《生成式人工智能服务管理办法（征求意见稿）》的配套标准；拟对生成式人工智能产品预训练和优化训练数据来源的合法性进行具体规范，详细描述符合法律法规要求、不含侵犯知识产权内容、保护个人信息等方面的具体要求，阐释数据的真实性、准确性、客观性、多样性要求。
2	信息安全技术 生成式人工智能人工标注安全规范	制定	本标准拟针对生成式人工智能产品研制中人工标注环节的标注规则、标注人员培训、标注内容正确性等方面提出安全规范。	本标准是《生成式人工智能服务管理办法（征求意见稿）》的配套标准；拟针对生成式人工智能产品研制中的人工标注环节，详细描述清晰、具体、可操作的人工标注规则，标注人员培训，标注内容正确性等方面的具体要求。
3	信息安全技术 大型网络平台网络安全评估指南	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，给出大型网络平台网络安全评估内容、评估方法、评估流程等方面的指导性信息。	本标准拟解决目前针对大型网络平台网络安全评估缺乏标准指导，有利于大型网络平台参考标准开展自评估，提升大型网络平台网络安全水平。

序号	标准名称	类型	主要内容	拟解决问题
4	信息安全技术 网络安全产品互联互通 告警信息格式	制定	本标准拟提出支持不同网络安全产品互联操作的告警信息格式、字段和内容描述。	本标准拟解决网络安全产品告警信息由于格式不统一带来的信息内容难以有效整合利用、同一事件重复告警导致应急处置效率较低等问题；适用于网络安全产品互联互通功能的设计、开发、应用和测试。
5	信息安全技术 网络安全产品互联互通 资产信息格式	制定	本标准拟提出支撑不同网络安全产品互联操作的网络资产信息格式、字段和内容描述。	本标准拟解决当前网络安全产品资产描述不统一、资产信息不准确带来的网络安全信息难以高效、合理利用的问题；适用于指导网络安全产品互联互通功能的设计、开发、应用和测试。
6	信息安全技术 数据分类分级保护要求	制定	本标准拟给出数据分类分级保护要求。	本标准在数据分类分级规则的基础上，进一步明确分类分级保护要求，支撑《数据安全法》第二十一条数据分类分级保护制度落地。
7	信息安全技术 个人信息保护合规审计指南	制定	本标准拟提出个人信息保护合规审计的实施流程和审计内容。	支撑《个人信息保护法》第五十四条、第六十四条关于个人信息处理活动进行合规审计的要求；适用于指导个人信息处理者和专业机构开展个人信息保护合规审计工作。
8	信息安全技术 个人信息可携带技术要求	制定	本标准拟给出个人信息可携带的原则、流程、方式等规则，以及安全保护要求。	本标准拟解决个人信息在转移、携带过程中遭到篡改、破坏、泄露等问题，防范个人信息被非法获取、非法利用。

序号	标准名称	类型	主要内容	拟解决问题
9	信息安全技术 互联网信息服务深度合成安全规范	制定	本标准拟从互联网信息服务生命周期的信息生成、处理、发布、传播、存储、销毁等环节，以及技术算法生命周期的设计开发、验证测试、部署运行、维护升级、退役下线等五个阶段，对深度合成服务提供者和技术支持者提出开展互联网深度合成服务在安全方面的通用要求以及证实评估方法。	本标准是支撑《互联网信息服务深度合成管理规定》的配套标准，细化补充管理规定各项要求，解决深度合成服务提供者对规定细化理解不到位，以及实践落实规定各项条款时执行不到位的问题。
10	信息安全技术 网络身份认证公共服务 应用接入规范	制定	本标准拟规定各类应用使用国家网络身份认证公共服务时应符合的总体安全要求、接口对接和应用接入审核要求以及相应测试方法。	支撑《反电信网络诈骗法》第三十三条“国家推进网络身份认证公共服务建设”的落地实施，保障各类应用通过国家网络身份认证公共服务对用户身份进行核验；适用于接入国家网络身份认证公共服务平台应用的开发、测试和验收。
11	信息安全技术 网络身份认证公共服务 小程序平台应用技术规范	制定	本标准拟规定小程序平台和运行在其上的小程序使用国家基础设施网络身份认证公共服务中的技术要求和安全要求。	为解决小程序及相应平台在使用国家基础设施网络身份认证公共服务中高效性、安全性，本标准指出小程序及其平台在设计、开发中的技术、安全要求。保障了国家基础设施对小程序及其平台开展服务的能力。适用于小程序平台和运行在其上的小程序使用网络身份认证公共服务的设计和开发。

序号	标准名称	类型	主要内容	拟解决问题
12	信息安全技术网络空间地理图谱要素表示要求	制定	本标准拟从网络空间地理图谱的要素分类与代码、图形符号表达和图谱构建三个方面，明确网络空间要素的类别、等级和代码，规定网络空间地理图谱符号的定义规范、使用原则和图形化表达，提供网络空间地理图谱构建的框架性参考。	本标准解决当前网络空间地理图谱缺乏统一框架及技术要求等问题；适用于规范网络安全部门开展网络安全资产管理、网络安全综合防控等工作，指导政府、高校、企业等机构开展网络空间的研究工作。
13	信息安全技术网络安全运营实施指南	制定	本标准拟提出网络安全运营参考框架，规范预测、防御、监测和响应等网络安全运营实施内容，以及网络安全运营效果评估模型与效果度量指标。	本标准拟解决网络安全人员、设备、流程、机制等缺乏统筹协调，未能形成防护合力，且运营效果缺乏评价；安全运营模式各不相同，关键技术要求缺乏定义，指标缺乏统一等问题。
14	信息安全技术数据接口安全风险监测方法	制定	本标准拟对数据接口面临的安全风险进行分类，明确风险监测的基本原则，从监测信息字段、流量采集方式、风险判定机制等方面提出技术要求和实施方法。	本标准拟解决数据接口利用过程中，导致数据泄露、滥用等问题；增强数据接口的安全风险预警和防护能力。

序号	标准名称	类型	主要内容	拟解决问题
15	信息安全技术数字水印技术实现指南	制定	本标准拟提出数字水印技术的概述、算法、流程、接口、原则，以及在图像、视频、文件、数据库等水印载体中的实现建议。	本标准拟解决由于缺乏统一的实施流程、服务接口等，导致的数字水印技术可靠性和可信性不足问题；也可为数据处理者应用数字水印技术实现数据版权保护、数据泄露追踪溯源。
16	信息安全技术数据安全和个人信息保护社会责任指南	制定	本标准拟提出数据安全和个人信息保护社会责任履行的内部管理机制、技术创新、公平运行、消费者权益保护、社会发展等方面社会责任的议题描述、相关行动和期望，以及评价方法。	本标准拟解决目前互联网平台等组织社会责任履行情况不明，社会责任履行情况未披露或披露内容中与数据安全和个人信息保护关联度低等问题；适用于组织识别和开展数据安全和个人信息保护社会责任相关活动，以及第三方机构评价组织在履行数据安全和个人信息保护社会责任的水平。
17	信息安全技术标识密码认证系统密码及其相关安全技术要求	制定	本标准拟给出基于SM9标识密码算法的密钥管理系统的完整架构，包含组成说明、功能要求和技术要求；给出标识密钥的申请、生成、签发、下载等基本功能要求和操作流程，同时对密钥管理系统的层次结构定义。	本标准拟解决基于SM9算法的密钥管理系统在设计、建设和使用中的关键技术问题,包括系统组成部分之间的关系、初始化过程以及各功能流程的具体实现,用于指导基于SM9算法的密钥管理基础设施的设计、建设。

序号	标准名称	类型	主要内容	拟解决问题
18	信息安全技术公钥密码应用技术体系框架	制定	本标准拟规定公钥密码应用技术体系框架，包括密码设备服务层、通用密码应用支撑层、典型密码应用支撑层和基础设施安全支撑平台等四部分的层次结构和逻辑关系，各层次的作用和内容，以及该体系框架内的密码标准的关系。	建设公钥密码应用技术体系的目的是：使密码算法、密码协议有机结合、共同作用，达到密码安全保障目的；使密码产品、密码服务、密码基础设施和技术标准相互配套、共同支撑，有效发挥密码技术作用；向应用系统提供与具体密码算法、密码协议、密钥管理、密码设备无关的、统一的密码服务，解决密码服务的共性支撑保障问题；为密码标准体系构建提供基础支持。
19	信息安全技术异步区块链共识机制安全规范	制定	本标准拟明确异步区块链共识机制的安全目标、系统边界和对外接口；给出异步共识机制的通用框架和具体实现方法，规定其采用的密码技术；规范异步共识机制的性能和安全性测评方法。	本标准拟解决同步和半同步共识机制在网络带宽波动大、通信延迟难以预测的异步环境中缺乏安全性保障的问题，指导各类联盟链场景采用异步共识机制实现区块链的一致性和活性。
20	信息安全技术半同步区块链共识机制安全规范	制定	本标准拟给出区块链共识协议技术规范，围绕区块链的安全性和功能需求，明晰共识协议的安全模型与安全目标、技术架构、角色交互框架以及交易处理流程；给出安全高效的共识机制具体方案；规范共识协议测评方法。	本标准拟解决区块链共识系统节点动态变化产生的系统安全问题和效率影响问题，指导各类区块链场景下采用区块链共识协议管理区块链共识节点准入授权及处理链上交易。

序号	标准名称	类型	主要内容	拟解决问题
21	信息安全技术 网络安全试验平台 体系架构	制定	本标准拟规定网络安全试验平台的参考架构，分别从参考体系架构、分系统基本功能、安全性保障方面进行阐述。	本标准拟解决国内网络安全试验平台建设技术标准不统一，不规范的问题；适用于国内网络安全试验平台的设计、建设、运营。
22	信息技术 安全技术 网络安全 第 6 部分:无线网络访问安全	制定	本标准等同采用 ISO/IEC 27033-6:2016；拟规定与无线网络相关的威胁、安全要求、安全控制和设计技术。	本标准拟解决无线网络访问安全问题；为选择、实施和监测使用无线网络提供安全通信所必需的技术控制提供指南。
23	信息技术 安全技术 网络安全 第 7 部分: 网络虚拟化安全	制定	本标准等同采用 ISO/IEC 27033-7; 拟规定网络虚拟化安全的威胁、安全要求、安全控制、设计技术和考虑。	本标准拟解决网络虚拟化带来的信息泄露、DDos 攻击、内容伪造、网络可用性降低等安全问题，为组织构建安全的虚拟化环境提供指导。
24	信息安全技术 信息系统灾难恢复规范	修订	本标准拟修订 GB/T20988—2007 和 GB/T30285—2013，拟规定灾难恢复工作应遵守的准则、上层规范架构，灾难恢复中心包括灾难恢复系统的规划、设计、实施、维护和恢复等全生命周的技术与管理规范。修订内容包括在原标准基础上，进一步明确目前灾难恢复全生命周工作的技术细节，明确评价方法、细化规范内容。	本标准拟解决灾难恢复领域中灾难恢复中心、灾难恢复系统规划、设计、建设、维护和恢复的全生命周期功能性、安全性、稳定性问题，为灾难恢复工作涉及的各方角色提供科学的技术和管理规范。

序号	标准名称	类型	主要内容	拟解决问题
25	信息安全技术公钥基础设施时间戳规范	修订	本标准拟修订 GB/T 20520-2006，拟规定时间戳部件组成、时间戳的管理、时间戳的格式和时间戳系统安全管理等方面的要求。	针对当前 PKI 系统、抗抵赖服务和日志审计系统等密码应用中时间戳缺少标准实现的问题，本标准通过提出适合国密算法应用的时间戳规范，确保时间戳产品和服务的安全性、互操作性和时间可信性，满足当前密码应用对于可信时间戳的需求。
26	信息安全技术公钥基础设施 PKI 组件最小互操作规范	修订	本标准拟修订 GB/T 19771-2005，拟对证书、证书撤销列表（CRL）扩展等术语进行描述，并对证书申请、更新、撤销、从资料库检索证书和 CRL 等内容提出相关要求。	本标准拟解决当前版本标准技术内容与国密算法体系存在差异的问题；同时，支持双证书体系监管和备份等 PKI 密钥管理需求。
27	信息安全技术公钥基础设施证书管理协议	修订	本标准拟修订 GB/T 19714-2005，拟描述公钥基础设施（PKI）中的证书管理协议，拟定义与证书产生和管理相关的各方面所需要的协议消息，消息主要包括申请证书、撤销证书、密钥更新、密钥恢复、交叉认证等。修订内容包括补充执行协议细节，补充协议参考报文等内容。	本标准拟解决当前版本标准缺少国密算法标识和使用方法等内容。如标准未说明双证书签发如何组装请求与对应响应，导致 CA 厂商处理方式各不相同；标准中协议结构缺少细节内容，导致 CA 厂商无法有效衔接。

序号	标准名称	类型	主要内容	拟解决问题
28	信息安全技术 信息安全管理体系 要求	修订	该标准修订 GB/T 22080-2016，等同采用 ISO/IEC 27001:2022，拟规定在组织环境下建立、实现、维护和持续改进信息安全管理体系的要求。	本标准拟解决组织信息安全问题 ，支撑信息安全管理体系（ISMS）的落地实施。
29	信息安全技术 信息安全风险管理指导	修订	本标准等同采用 ISO/IEC 27005:2022，拟规定组织开展信息安全风险管理活动所需的过程及实施指南。	本标准拟为组织开展信息安全风险管理活动提供指导，并满足 ISMS 有关应对信息安全风险活动的要求。
30	信息安全技术 云计算服务安全能力评估方法	修订	本标准修订 GB/T 34942—2017，拟给出依据 GB/T 31168《信息安全技术 云计算服务安全能力要求》开展安全能力评估的原则、实施过程以及针对各项具体安全要求进行评估的方法。	本标准拟解决对云服务进行安全能力评估时面临的评估方法和手段不统一的问题。