附件 1

2022 年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 重要数据处理安全要求	制定	本标准拟明确数据处理者在重要数据全流程处理过程中的保护要求，重点针对存储、使用环节提出专门要求。	支撑《数据安全法》第二十一条对重要数据进行重点保护的要求。
2	信息安全技术 数据安全风险评估方法	制定	本标准拟明确数据安全风险评估的方法、流程、评估报告编制等内容。	支撑《数据安全法》第十八条、第三十条对数据安全风险评估相关规定的落地实施。
3	信息安全技术 政务数据处理安全要求	制定	本标准拟规范政务部门自行和委托第三方开展的政务数据处理活动，明确政务数据处理安全管理要求、安全技术要求及对各类数据处理者的安全监督要求，重点针对共享环节提出专门要求。	支撑《数据安全法》第三十九条、第四十条关于保障政务数据安全相关规定的落地实施。

序号	标准名称	类型	主要内容	拟解决问题
4	信息安全技术 公共数据开放安全要求	制定	本标准拟明确公共数据面向社会开放时个人信息保护要求，如个人信息应脱敏后向社会开放；数据开放的技术要求，如部分数据可以通过直接提供数据的方式开放，部分数据只开放数据的使用权，数据不直接提供给使用方；数据开放的管理要求，例如企业和群众提出开放数据侵犯其权益的处理要求等。	支撑《数据安全法》第七条、第四十二条关于国家构建统一规范、互联互通、安全可控的政务数据开放平台的建设、运行。
5	信息安全技术 敏感个人信息处理安全要求	制定	本标准拟针对医疗健康、金融账户、行踪轨迹等敏感个人信息，明确数据处理者进行收集、存储、使用、加工、传输、提供、公开、删除等处理活动的安全要求，重点针对采集必要性、安全保护、脱敏规则、告知同意等方面提出要求。	支撑《个人信息保护法》第二节敏感个人信息的处理规则的落地实施。

序号	标准名称	类型	主要内容	拟解决问题
6	信息安全技术 基于个人信息的自动化决策安全要求	制定	本标准拟明确数据处理者在进行自动化决策及相关应用过程中的数据安全和个人信息保护要求。	支撑《个人信息保护法》第二十四条对利用个人信息进行自动化决策的要求的落地实施。
7	信息安全技术 大型互联网企业个人信息保护监督机构要求	制定	本标准拟明确提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的范围，大型互联网企业外部监督机构人员选择、人员结构、人员资质、人员约束、运行机制等要求。	支撑《个人信息保护法》第五十八条第一款对“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”“按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督”等相关规定的落地实施。

序号	标准名称	类型	主要内容	拟解决问题
8	信息安全技术 数据安全评估机构能力要求	制定	本标准拟明确数据安全评估机构和人员管理要求、资格评定、技术能力等相关要求。	支撑《数据安全法》第十八条“国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动”规定的落地实施。
9	信息安全技术 个人信息跨境传输认证要求	制定	本标准拟明确个人信息跨境提供的安全原则、安全要求和认证规则。	支撑《个人信息保护法》第三十八条个人信息跨境提供安全认证工作。
10	信息安全技术 网络安全产品互联互通框架	制定	本标准拟提出网络安全产品互联互通框架和接口要求，指导网络安全产品互联互通的设计、开发和应用。	本标准拟解决网络安全产品在互联互通方面由于接口和数据格式差异导致的难以有效协同问题。
11	信息安全技术 IPv6 地址编码规则	制定	本标准拟给出IPv6的地址编码规则。	本标准拟解决 IPv6 大规模应用部署过程中面临的地址编码不恰当设置、海量地址安全检测难度高等安全风险。

序号	标准名称	类型	主要内容	拟解决问题
12	信息安全技术 开源软件安全评价准则	制定	本标准拟提出针对开源软件的安全性评价指标和评价方法。	本标准拟解决开源软件安全风险传播性强、防控性弱、应对性差等问题。
13	信息安全技术 关键信息基础设施安全测评要求	制定	本标准拟规定关键信息基础设施分析识别、安全防护、检测评估、监测预警、主动防御、事件处置等环节的安全检测评估要求。	支撑《关键信息基础设施安全保护条例》的落地实施，为关键信息基础设施的安全测评工作提供方法和技术支撑。
14	信息安全技术 电子数据收集提取技术要求	制定	本标准拟规定电子数据收集提取的术语、定义、通用要求，以及收集提取的方法、步骤、记录和结果表述等技术规范。	本标准拟解决电子数据收集提取过程操作不规范，方法步骤不统一，记录与结果表述不一致等问题。

序号	标准名称	类型	主要内容	拟解决问题
15	信息安全技术 安全运维系统技术规范	制定	本标准拟规范安全运维系统的安全功能要求、安全保障要求和测试评价方法。	安全运维系统存储着资产管理账号、具备重要资源的访问权限等，一旦其自身存在安全短板将会为重要信息系统和关键信息基础设施引入极大的安全风险。本标准的制定将紧密贴合重要信息系统及关键信息基础设施安全运维和资产管理的合规性需求，旨在降低运维管理安全风险。
16	信息安全技术 数据安全交换产品技术规范	制定	本标准拟规范数据安全交换产品的安全功能要求、安全保障要求和测试评价方法。	本标准拟解决在不同类别数据的交换过程中数据泄露、被攻击的风险，为不同网络间、不同云间、大数据的不同平台之间提供安全的数据交换。

序号	标准名称	类型	主要内容	拟解决问题
17	信息安全技术 互联网恶意软件定义与描述格式	制定	本标准拟描述互联网恶意软件样本的定义及分类，拟规范关于捕获来源、行为、危害等属性的描述格式。	本标准拟解决互联网恶意软件治理工作中对恶意软件的判定命名及描述问题，主要包括：互联网恶意软件的定义和边界不清晰、互联网恶意软件的恶意行为分类混乱并缺乏对应的判定依据、互联网恶意软件的衍生信息定义格式不统一以及恶意软件的描述格式缺乏统一等问题。
18	信息安全技术 网络安全保险应用指南	制定	本标准拟提出不同组织在选择和使用网络安全保险来降低网络安全风险时应考虑的主要内容，对网络安全保险的保障范围、如何选择保险方，以及如何通过风险评估来支持网络安全保险等提出指导性信息。	本标准拟解决组织对网络安全保险缺乏统一理解，对网络安全风险和保险保障范围认知差异较大，以及如何利用网络安全保险进行控制部分风险等问题。

序号	标准名称	类型	主要内容	拟解决问题
19	信息安全技术 机密计算通用框架	制定	本标准拟定义机密计算技术的核心组件、接口和必要属性及环境创建过程。	机密计算的使用需要上层应用和底层平台配合才能实现，但由于不同平台厂商机密计算的基础组件间交互方式及接口的定义不同，导致不同平台厂商之间的技术无法互通，引发应用跨CPU平台无法使用问题。
20	信息安全技术 人工智能计算平台安全框架	制定	本标准拟提出人工智能计算平台安全框架以及相应的安全模块和机制，以保障用户数据与人工智能模型数据安全。	本标准拟解决 AI 应用开发运行过程面临的底层硬件安全问题，以及上层应用面临的多场景基础共性安全问题，保护 AI 模型及数据。
21	信息安全技术 数据交易服务安全要求	修订	本标准拟修订 GB/T 37932—2019，拟明确数据交易的参与方、交易对象和交易过程的安全要求。	支撑《数据安全法》第十九条关于规范数据交易行为相关规定的落地实施。

序号	标准名称	类型	主要内容	拟解决问题
22	信息安全技术 办公设备安全规范	修订	本标准拟修订 GB/T 29244—2012 和 GB/T 38558—2020，拟规定办公设备的安全技术要求和测试评价方法。主要修改内容包括在原标准基础上增加办公设备在驱动程序、固件、数据、供应链等方面的安全要求和对应测评方法。	本标准拟解决办公设备安全性问题，针对办公设备在主控芯片、存储、耗材、供应链等方面面临的安全风险，提出安全技术要求和对应测评方法。
23	信息安全技术 网络安全服务能力要求	修订	本标准拟修订 GB/T 32914—2016，拟规范网络安全服务机构在提供网络安全服务时应具备的能力。	支撑《网络安全法》第三十八条，《关键信息基础设施安全保护条例》第十七条、第三十七条的落地实施。本标准拟解决检测评估、安全运维等服务质量参差不齐、缺乏可持续性、服务工具供应链安全存在隐患等导致服务需求方利益受损问题，以及关键信息基础设施运营单位安全服务过程中存在缺少人员背景审查、敏感数据泄露、重要系统被控制等安全风险。

序号	标准名称	类型	主要内容	拟解决问题
24	信息安全技术 散列函数 第1部分:概述	修订	本标准拟修订 GB/T 18238.1—2000，拟规定GB/T 18238系列使用的术语、定义、符号和要求等，主要修改内容包括散列函数的一般模型和填充方法等。	本标准拟解决散列函数的统一描述问题，规范散列函数的描述方法，指导本标准后续部分规定具体的散列函数。
25	信息安全技术 散列函数 第2部分:采用 n 位块密码的散列函数	修订	本标准拟修订 GB/T 18238.2—2002，拟规定采用分组密码算法构造散列函数的方法，主要修改内容包括遴选并规定具体方法，补充测试向量等。	本标准拟解决采用分组密码算法构造散列函数的方法问题，指导部分场景中使用分组密码算法提供数据完整性保护等。
26	信息安全技术 散列函数 第3部分:专用散列函数	修订	本标准拟修订 GB/T 18238.3—2002，拟规定专用散列函数，主要修改内容包括遴选并规定专用散列函数，描述构造模型，补充测试向量等。	本标准拟解决专用散列函数的定义和算法描述问题，指导各类场景采用专用散列函数保护数据完整性等。

序号	标准名称	类型	主要内容	拟解决问题
27	信息安全技术 实体鉴别 第 2 部分: 采用对称加密算法的机制	修订	本标准拟修订 GB/T 15843.2-2017，修改采用 ISO/IEC 9798-2:2019，拟在采用对称算法的各个实体鉴别机制中，以可鉴别的加密来代替加密；增加可唯一标识每个机制中的可鉴别加密实例的常数；适应性修改部分术语和定义、章节标题等内容。	本标准拟通过分析不同机制下采用可鉴别加密，实现实体鉴别的安全性和适用性，并对相关方及其信息交互进行明确规定，解决网络空间隐私保护问题。
28	信息安全技术 消息鉴别码 第 2 部分: 采用专用杂凑函数的机制	修订	本标准拟修订 GB/T 15852.2-2012，修改采用 ISO/IEC 9797-2:2021，拟修改可选杂凑函数的范围，规范采用我国 SM3 密码杂凑算法的消息鉴别码算法，并相应修改算法描述与常数的计算；增加关于 MAC 值和输出数据串长度限制的说明；增加 MAC 算法概述、密钥长度、输入数据比特串长度的说明；修改部分术语和定义、章节标题等，增强系列标准规范化。	本标准拟解决消息被篡改、伪装成发送者发送消息等问题。

序号	标准名称	类型	主要内容	拟解决问题
29	信息安全技术 公钥基础设施 在线证书状态协议	修订	本标准拟修订 GB/T 19713-2005，拟增加 SM2 和 SM3 算法相关的标准引用；根据 RFC 6960 补充和修订内容，增加 OCSP 请求和响应的证书状态的扩展、签名算法的扩展等数据的补充说明；在客户端请求中增加客户端期望响应使用的签名算法，OCSP 的响应支持多签名算法；参照 RFC5019，增加对移动互联网，采用轻量级协议；参照 RFC8954，增加 Nonce 扩展。	本标准拟通过向应用提供一种无需请求证书撤销列表(CRL)即可查询数字证书状态的机制，让国密 SM2 算法应用、移动互联网应用及时获得证书撤销状态的有关信息。
30	信息安全技术 网络和终端隔离产品技术规范	修订	本标准拟修订 GB/T 20277—2015 和 GB/T 20279—2015，拟规定网络和终端隔离产品的安全技术要求和测试评价方法。修订内容包括在原标准基础上，明确产品分类，增加应用协议、集群部署等新的安全技术要求和测评方法，并细化性能要求。	本标准拟解决网络和终端隔离产品面对不同协议、不同场景和不同攻击类型的安全问题。

序号	标准名称	类型	主要内容	拟解决问题
31	信息安全技术 终端计算机通用安全技术规范	修订	本标准拟修订 GB/T 29240—2012，结合可信计算技术，拟从安全功能要求、自身安全保护、设计与实现、安全管理4个维度提出了5个等级的终端计算机安全技术要求，并给出了相应的测试评价方法。	本标准拟解决终端计算机面临的病毒攻击、恶意攻击和数据失窃等问题。
32	信息安全技术 政务计算机终端核心配置规范	修订	本标准拟修订 GB/T 30278—2013 和 GB/T 35283—2017，拟规范政务计算机终端的操作系统、办公软件、浏览器、邮件系统、BIOS 系统、防护软件等核心基础软件的安全配置要求，加强终端核心防护能力，并规范核心配置的自动化实现方法及实施流程。	本标准拟解决大规模终端自动化安全配置问题，提升终端安全基准和安全防护能力。

序号	标准名称	类型	主要内容	拟解决问题
33	信息安全技术 存储介质数据恢复服务要求	修订	本标准拟修订 GB/T 31500—2015，拟规定实施存储介质数据恢复服务所需的服务安全原则、服务管理安全要求、服务实施安全要求及评价办法。该标准适用于指导提供存储介质数据恢复服务机构针对非涉及国家秘密的数据恢复服务安全实施和管理。	本标准拟解决数据恢复服务行业存在技术和管理安全问题，主要包括：行业作坊式特点明显，存在很多管理和技术安全风险；行业诚信度不够，缺乏数据恢复从业者、从业者、从业环境的规范；数据恢复服务质量不好衡量，缺乏评价体系等问题。
34	信息安全技术 信息安全控制实践指南	修订	本标准拟修订 GB/T 22081—2016，拟为组织的信息安全标准和信息安全管理实践提供指南，在考虑组织信息安全风险环境下提出信息安全控制的选择、实现和管理。	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。