

国家标准《信息安全技术 重要数据识别指南》

（征求意见稿）编制说明

一、工作简况

1.1 任务来源

《信息安全技术 重要数据识别指南》是国家标准化管理委员会下达的信息安全国家标准制定项目。该项目由中电数据服务有限公司牵头负责（负责人左晓栋、周亚超），并联合杭州安恒信息技术股份有限公司、国家工业信息安全发展研究中心等 20 余家单位编制。2021 年 5 月，国家标准化管理委员会下达了国家标准计划号 20210995-T-469。该标准由全国信息安全标准化技术委员会提出并归口。

1.2 编制单位

本标准由中电数据服务有限公司牵头，北京理器科技有限公司、杭州安恒信息技术股份有限公司、国家工业信息安全发展研究中心、北京信息安全测评中心、清华大学、中国信息安全测评中心、公安部第三研究所、国家计算机网络应急技术处理协调中心、国家信息中心、中国软件评测中心、中国网络安全审查技术与认证中心、国家信息技术安全研究中心、中国信息通信研究院等单位共同参与编制，归口单位为全国信息安全标准化技术委员会。

1.3 工作过程

1.3.1 成立编制组

接到标准编制任务后，中电数据服务有限公司联合数据安全领域科研机构、检测机构、高校、律所、互联网企业、安全厂商以及其他数据密集型企业组建标准编制组，编制组成员具有丰富的标准编制经验、数据安全保护领域研究经验。

1.3.2 制定工作计划

编制组首先制定了编制工作计划，并确定了编制组人员例会安排以便及时沟通交流工作情况。

1.3.3 研究国内外政策标准资料

该标准编制过程中，一方面充分借鉴了国外在行业管理、特定事项中对数据

（非个人信息、非涉密信息）的管理经验，包括对非个人特定数据（重点场所的安保数据、商业领域知识产权、出口管控项等）的管理要求；对非个人特定数据的分类标准，如 NIST SP 800-60《将各类信息与信息系统映射到安全类的指南》；美国对受控非密信息的管理要求和相关标准，包括第 13556 号行政令《受控非密信息》，以及 NIST SP 800-171 系列标准。另一方面，落实我国数据安全政策法规要求，切实反映中国国情和管理需要，体现中国政府治网理念和关于数据安全的立场主张，研究当前我国对重要数据提出的管理要求，如《网络安全法》《数据安全管理办法（征求意见稿）》《网络安全审查办法》等；参考关于重要数据识别的前期研究基础；结合我国现有行业数据管理要求，包括测绘地理信息、地震数据、人类遗传资源、科学数据、健康医疗数据、金融数据、教育数据、央企数据、国防军工数据、气象数据、药品数据、工业数据、公共数据等。

1.3.4 编制工作简要过程

按照项目进度要求，编制组人员首先对相关法律法规及国内外标准文件进行反复阅读与理解，查阅有关资料，编写标准编制提纲，在完成对提纲进行交流和修改的基础上，开始具体的编制工作。

2020 年 3 月，与标准编制组现有主要单位基于前期研究项目成果进一步开展广泛调研，研读国内外相关政策和标准文件，形成标准草案第一稿，开展标准申报。

2020 年 5 月，标准经全国信息安全标准化技术委员会工作组“会议周”讨论通过，获得立项。

2020 年 7 月-9 月，接到全国信息安全标准化技术委员会标准制定任务后，经公开征集参编单位正式成立标准编制组。牵头单位随即召集标准编制组成员具体讨论和分配了小组任务。

2020 年 10 月，经广泛征求意见，根据我国最新数据安全政策法规对标准草案第一稿进行修改，调整标准框架，形成标准草案第二稿。

2020 年 10 月 11 日，参加 2020 年网络安全国家标准重点项目检查会，会后编制组开会讨论，形成标准草案第三稿。

2020 年 11 月 6 日上午，通过线上会议形式正式召开项目启动会，明确后续标准编制思路、重点研究内容及需注意的事项。

2020年11月6日下午，参加全国信息安全标准化技术委员会大数据组组织的专家评审会，根据专家意见修改形成标准草案第四稿。

2020年11月12日，编制组将草案提交2020年第二次标准会议周讨论，形成征求意见稿。编制组针对会议周工作组成员提出的意见建议，专题组织研讨，对标准征求意见稿进行修改完善。

2020年12月-2021年3月，根据信安标委秘书处审核意见进一步完善征求意见稿。

2021年3月25日，参加2020年网络安全国家标准重点项目检查会，会后编制组开会讨论，根据专家意见修改征求意见稿。

2021年5月10日，编制组在2021年第一次标准会议周上汇报项目进展情况。会后，针对工作组成员提出的意见建议组织专题研讨，对标准征求意见稿进行修改完善。

2021年6月25日，参加全国信安标委秘书处组织的2020年网络安全国家标准项目抽查会。会后针对专家提出的意见建议修改标准征求意见稿。

2021年6月29日，编制组邀请相关部门领导、行业专家对标准文本进行研讨，阐述标准编制思路和重点考虑，会后，根据讨论情况完善标准文本。

2021年11月，在2021年第二次标准会议周上汇报项目进展情况。会后，针对工作组成员提出的意见建议组织专题研讨，对标准征求意见稿再次进行修改完善。

2021年12月15日，全国信安标委秘书处与标准编制组进行专门研讨，针对一段时间以来各方面的反映和期盼，结合《网络数据安全条例》等法律法规制定进展，提出了调整标准编制思路的建议。会后，根据秘书处建议，对标准征求意见稿作了较大修改。

2022年1月7日，全国信安标委秘书处组织召开评审会，对标准进行了阶段性评审。根据会上专家意见，编制组形成正式征求意见稿，向社会公开征求意见。

二、标准编制原则和确定主要内容的论据及解决的主要问题

随着数据成为国家基础性战略资源，其安全保护成为国家网络安全工作的一项重点。除涉密信息和个人信息外，还有一部分数据十分重要和敏感，即重要数

据，其一旦被泄露、损毁、篡改、滥用，可能会带来严重后果，危害国家安全与公共利益。

这些数据可能分布在政务部门（宏观经济数据、金融监管数据、人口资源数据、健康数据、执法数据、交通运输数据等），关键信息基础设施运营者在内的重点行业企业（金融交易数据、能源生产和消费数据、关键信息基础设施资产数据、网络安全防护信息等），医院、高校等公共服务机构（健康医疗数据、教育数据等），具有相应资质或承担特定职能的权威专业机构（地理、地震、天文、气象等科学数据及其衍生数据等），科研机构（科研成果及其相关数据、知识产权等），互联网企业（在线提供导航、电子商务、即时通信等服务时收集、产生的，涉及经济、地理、人口、法人等国家基础信息的数据）或实体经济企业（大型工程施工设备导航和无线通信模块传输的敏感工程物理位置、施工土石方等）。

近年来，我国已多次提出相关保护要求，但此前，重要数据的定义、范围和识别方法没有定论，对重要数据的识别方法和途径尚未形成实践指引。2021年11月14日，国家互联网信息办对《网络数据安全条例》公开征求意见，提出了重要数据的定义，并设立了一系列重要数据安全监管制度，使重要数据的识别问题成为影响当前国家数据安全工作进展的重大议题。

本标准拟解决重要数据安全管理的适用对象和适用范围问题。标准编制过程中，一方面充分吸收国内外重要数据安全保护经验，参考 NIST SP 800-60《将各类信息与信息系统映射到安全类的指南》、NIST SP 800-171《保护非联邦系统和机构的受控非密信息》等国外指南，并重点借鉴了 NIST SP 800-59《国家安全系统识别指南》，另一方面注重落实我国《网络安全法》《网络安全审查办法》及相关法律法规和政策文件中关于重要数据的有关规定，分析重要数据的属性、面临的威胁和主要分布情况，提出与国际标准接轨、适合我国国情，具有可操作性的重要数据的识别过程和方法，为各部门、各行业制定本部门、本领域的重要数据清单提供指导，为加强重要数据管理安全管理提供支撑。

制定本标准的原则是：

- **聚焦国家安全，避免范围扩大。**重要数据主要从国家安全、公共利益等角度衡量，其范围应当尽可能小，不包括企业生产经营和内部管理信息、个人信息等。我国对涉密信息的安全保护已有明确工作制度，“重要数据”

不包括涉密信息。但分布在商业领域和企业系统中的有些数据可能属于重要数据。对于行业主管部门已经制定实施数据管理政策和标准规范的，重要数据的识别应当从其规定。

- **遵循国际惯例，反映中国特色。**立足开放环境维护网络安全，着眼全球化发展需要，促进数据安全有序流动，充分借鉴国外已有做法，推动网络空间命运共同体建设。同时，针对国内蓬勃发展的移动互联网应用、日益丰富的互联网业态等情况，反映中国国情和管理需要，体现中国政府治网理念和关于数据安全的立场主张。
- **定性定量结合，突出可操作性。**以定性与定量相结合的方式识别重要数据，根据具体情况采取不同识别方法。某些数据，其所在行业、应用领域决定了本身的重要性。但也有某些数据，在一般情况下不属于重要数据，但在达到一定量后产生质变，此时需要对重要数据进行定量描述。

三、主要试验[或验证]情况分析

标准由国家工业信息安全发展研究中心牵头开展应用推广。国家工业信息安全发展研究中心是工业信息安全产业发展联盟、中关村信息技术和实体经济融合发展联盟（原两化融合服务联盟）等行业组织的理事长单位。其中，工业信息安全产业发展联盟是在工业和信息化部指导下，由中心与能源、化工、钢铁、有色、装备制造、石油、烟草、交通、电子制造、工业互联网平台、工业互联网安全、信息安全等领域的 45 家单位联合发起成立。目前，联盟已有 300 余家成员单位，形成了标准组、工业互联网安全组、测试评估组、应急服务组、人才促进组、产业应用组等完善的业务工作体系，其桥梁纽带作用和丰富的“产学研用”资源有助于面向重要行业领域组织开展标准的试点应用与验证，进一步加强标准内容的科学性、合理性，安全性、完备性和可操作性。

2021 年 4 月 1 日，参加全国信安标委秘书处组织的 15 项 2020 年重点标准试点工作启动会。会后，编制组制定试点方案，启动标准试点工作，包括启动、实施和总结三个阶段：

试点启动阶段：2021 年 4 月 30 日至 5 月 30 日，确定试点行业和专家组。召开试点工作启动会，邀请试点单位、编制组成员单位和专家组参加，对标准试点工作进行研讨与部署，确定在工控行业开展试点工作。

试点实施阶段：2021 年 6 月 1 日至 7 月 20 日。6 月 1 日至 10 日，编制组会

同相关专家，根据《指南》研究并确定工控领域重要数据识别的具体要求和实施细则；6月10日至7月10日，组织并遴选部分有意愿的工业信息安全产业发展联盟成员单位开展重要数据识别工作，并反馈识别结果。7月10日至20日，编制组会同行业专家根据反馈结果进行评估和总结。

总结阶段：2021年7月20日至7月30日。召开试点工作成果专家评审会，总结标准试点工作的成效和经验，评估标准的适用性、科学性等，并提出标准改进建议，以及为重要数据识别工作推进提出建议。

四、知识产权情况说明

本标准不涉及专利。

五、产业化情况、推广应用论证和预期达到的经济效果

重要数据识别指南的制定将为我国数据安全保护特别是重要数据安全管理工作提供基本依据，有助于防范数据安全重大风险、完善我国网络安全顶层设计，具有重大社会效益。

标准提出了重要数据的特征，明确了识别重要数据的基本流程以及对重要数据的描述格式，有助于数据出境安全评估制度的科学实施，从而便利数据跨境流动、促进国际贸易，有利于经济发展与国际合作。

六、采用国际标准和国外先进标准情况

本标准广泛调研了国内外相关政策标准，借鉴其他国家在行业管理、特定事项（如出口管控）中对数据（非个人信息）的管理经验，重点参考 NIST SP 800-60《将各类信息与信息系统映射到安全类的指南》、NIST SP 800-171《保护非联邦系统和机构的受控非密信息》、NIST SP 800-59《国家安全系统识别指南》等国外指南标准，同时注重落实我国《网络安全法》《网络安全审查办法》及相关法律法规和政策文件中关于重要数据的有关规定。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准符合现行法律法规要求，在编制过程中与相关标准保持协调一致。本项目旨在落实《网络安全法》第三十七条要求，是制定数据安全管理工作相关细则所必需的基础性标准，且与现有的强制性国家标准以及其他相关标准不重复、不冲突。

八、重大分歧意见的处理经过和依据

《信息安全技术 重要数据识别指南》编制过程中未出现重大分歧。

九、标准性质的建议

建议本标准作为推荐性国家标准发布实施。

十、贯彻标准的要求和措施建议

本标准给出了识别重要数据的基本原则、考虑因素、流程以及重要数据描述格式。

本标准为各地区、各部门制定本地区、本部门以及相关行业、领域的重要数据具体目录提供参考，为重要数据安全保护工作提供支撑，也可供各类组织在识别本组织重要数据时参考。

十一、替代或废止现行相关标准的建议

无。

十二、其它应予说明的事项

无。

国家标准《信息安全技术 重要数据识别指南》编制工作组

2022-1-1