ICS 35.030

CCS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 重要数据识别指南

Information security technology - Guideline for identification of critical data

（征求意见稿）

（本稿完成时间：2022 年 1 月 7 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中电数据服务有限公司、北京理器科技有限公司、杭州安恒信息技术股份有限公司、中国电子技术标准化研究院、清华大学、北京时代新威信息技术有限公司、国家工业信息安全发展研究中心、北京信息安全测评中心、中国网络安全审查技术与认证中心、中国信息安全测评中心、国家信息中心、中国软件评测中心、中国网络空间研究院、国家信息技术安全研究中心、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、中国信息通信研究院、交通运输部科学研究院、中国南方电网有限公司、数库（上海）科技有限公司、上海市方达律师事务所。

本文件主要起草人：左晓栋、吴梦婷、周亚超、张弛、郭晓雷、杨晓伟、赵慧、张誉鑫、吴迪、陈世翔、唐旺、王新杰、尹云霞、上官晓丽、金涛、崔占华、刘雨桁、吕华辉、柳彩云、杨帅锋、刘海峰、李媛、刘蓓、都婧、姜伟、崔聪聪、刘云、任卫红、袁静、林星辰、袁建廷、胡影、王惠莅、杨婷、杨韬、刘明辉、郭明多、刘彦、梁满。

信息安全技术 重要数据识别指南

1 范围

本文件给出了识别重要数据的基本原则、考虑因素以及重要数据描述格式。

本文件适用于数据处理者识别其掌握的重要数据，为重要数据安全保护工作提供支撑，也可供各地区、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。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069 中界定的以及下列术语和定义适用于本文件。

3.1

重要数据 critical data

以电子方式存在的，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

注：重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据。

4 识别重要数据的基本原则

识别重要数据遵循的原则如下：

a）聚焦安全影响：从国家安全、经济运行、社会稳定、公共健康和安全等角度识别重要数据，只对组织自身而言重要或敏感的数据不属于重要数据，如企业的内部管理相关数据；

b）突出保护重点：通过对数据分级，明确安全保护重点，使一般数据充分流动，重要数据在满足安全保护要求前提下有序流动，释放数据价值；

c）衔接既有规定：充分考虑地方已有管理要求和行业特色，与地方、部门已经制定实施的有关数据管理政策和标准规范紧密衔接；

d）综合考虑风险：根据数据用途、面临威胁等不同因素，综合考虑数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险，从保密性、完整性、可用性、真实性、准确性等多个角度识别数据的重要性；

e）定量定性结合：以定量与定性相结合的方式识别重要数据，并根据具体数据类型、特性不同采取定量或定性方法；

f）动态识别复评：随着数据用途、共享方式、重要性等发生变化，动态识别重要数据，并定期复查重要数据识别结果。

5 重要数据的识别因素

识别重要数据时，可考虑如下因素：

a）反映国家战略储备、应急动员能力，如战略物资产能、储备量属于重要数据；

b）支撑关键基础设施运行或重点领域工业生产，如直接支撑关键基础设施所在行业、领域核心业务运行或重点领域工业生产的数据属于重要数据；

c）反映关键信息基础设施网络安全保护情况，可被利用实施对关键信息基础设施的网络攻击，如反映关键信息基础设施网络安全方案、系统配置信息、核心软硬件设计信息、系统拓扑、应急预案等情况的数据属于重要数据；

d）关系出口管制物项，如描述出口管制物项的设计原理、工艺流程、制作方法等的信息以及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告属于重要数据；

e）可能被其他国家或组织利用发起对我国的军事打击，如满足一定精度要求的地理信息属于重要数据；

f）反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可能被恐怖分子、犯罪分子利用实施破坏，如反映重点安保单位、重要生产企业、国家重要资产（如铁路、输油管道）的施工图、内部结构、安防等情况的数据，以及未公开的专用公路、未公开的机场等的信息属于重要数据；

g）可能被利用实施对关键设备、系统组件供应链的破坏，以发起高级持续性威胁等网络攻击，如重要客户清单、未公开的关键信息基础运营者采购产品和服务情况、未公开的重大漏洞属于重要数据；

h）反映群体健康生理状况、族群特征、遗传信息等的基础数据，如人口普查资料、人类遗传资源信息、基因测序原始数据属于重要数据；

i）国家自然资源、环境基础数据，如未公开的水情信息、水文观测数据、气象观测数据、环保监测数据属于重要数据；

j）关系科技实力、影响国际竞争力，如描述与国防、国家安全相关的知识产权的数据属于重要数据；

k）关系敏感物项生产交易以及重要装备配备、使用，可能被外国政府对我实施制裁，如重点企业金融交易数据、重要装备生产制造信息，以及国家重大工程施工过程中的重要装备配备、使用等生产活动信息属于重要数据；

l）在向政府机关、军工企业及其他敏感重要机构提供服务过程中产生的不宜公开的信息，如军工企业较长一段时间内的用车信息；

m）未公开的政务数据、工作秘密、情报数据和执法司法数据，如未公开的统计数据；

n）其他可能影响国家政治、国土、军事、经济、文化、社会、科技、生态、资源、核设施、海外利益、生物、太空、极地、深海等安全的数据。

具备以上因素之一的，是重要数据。

6 重要数据描述格式

重要数据描述格式如表 1 所示。

a）基本信息

1）“处理者”指重要数据处理者；

2）“系统或应用”指重要数据所在的系统或所支撑的应用；

3）“地区或部门”指重要数据处理者所在的地区或部门。

b）分类

1）“类”指重要数据的类别，根据重要数据处理者所在地区、部门的规定确定；

2）“子类”指重要数据的子类别，视情况填写，有的重要数据还可对子类进一步细分。

c）重要性描述

1）“影响”指重要数据对国家安全、公共利益的影响，即重要数据之所以“重要”的理由；

2）“安全威胁”指重要数据在保密性、完整性、可用性、真实性、准确性等方面可能面临的安全威胁；

3）“重要性时效”指重要数据维持“重要性”的时间长度，时效过后便不再属于重要数据。

d）产生、使用与保护

1）“数量”指重要数据的量；

2）“来源”指重要数据如何收集或产生；

3）“用途”指使用重要数据的目的以及具体方式方法；

4）“共享情况”指与其他组织共享、交易、委托处理或向境外传输重要数据的情况；

5）“保护情况”指对重要数据采取的安全保护措施。

e）“备注”用于描述其他需要说明的事项。

表 1 重要数据描述格式

基本信息			分类		重要性描述			产生、使用与保护					备注
处理者	系统或应用	地区或部门	类	子类	影响	安全威胁	重要性时效	数量	来源	用途	共享情况	保护情况	

参考文献

[1] 《中华人民共和国保守国家秘密法》

[2] 《中华人民共和国网络安全法》

[3] 《中华人民共和国出口管制法》

[4] 《中华人民共和国数据安全法》

[5] 《中华人民共和国个人信息保护法》

[6] 《关键信息基础设施安全保护条例》

[7] NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories

[8] NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

[9] NIST SP 800-171A Assessing Security Requirements for Controlled Unclassified Information

[10] NIST SP 800-171B Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets