ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 重要网络数据识别指南

Information security technology - Identification guide of key cyber data

（草稿）

（本稿完成日期：2020-11-09）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1-2009《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。

本标准由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本标准起草单位：

本标准主要起草人：

信息安全技术 重要网络数据识别指南

1 范围

本标准提出了重要网络数据的识别过程和方法，描述了重要网络数据的特征。

本标准为各行业主管监管部门制定本行业的重要网络数据清单提供指导，为我国数据安全监督管理工作提供支撑。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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

政务信息 government affair information

政务部门在履行职责过程中收集或生成的，以一定形式记录、保存的文件、资料、图表等信息。

3.2

重要网络数据 key cyber data

指一旦泄露或被篡改、损毁可能直接影响国家安全、经济运行、社会稳定、公共健康和安全的，通过网络收集、产生或以电子形式存在的数据。

注：重要网络数据不包括国家秘密和个人信息。

3.3

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[GB/T 35273-2020，定义3.1]

4 重要网络数据识别基本原则

识别重要网络数据，应遵循以下原则：

a）聚焦国家安全：重要网络数据主要从国家安全、公共利益等角度衡量，其范围应尽可能小。重要网络数据并非对某个组织而言重要或敏感，企业生产经营和内部管理信息不属于重要网络数据。

b）促进数据流动：识别重要网络数据是为了明确数据安全保护和监管对象，目的是突出保护重点，规范数据开发利用，促进数据安全、有序流动。

c）反映行业特色：应考虑各行业特色，结合本行业对国家安全、公共利益等重要性识别重要网络数据。对于行业监管主管部门已经制定实施有关数据管理政策和标准规范的，重要网络数据的识别应当与其紧密衔接。

d）综合考虑风险：根据数据的用途、面临的威胁不同，重要网络数据的安全保护需求可能体现在保密性、完整性、可用性、真实性、准确性等方面，识别时应综合考虑数据被未经授权披露、丢失、滥用、篡改或销毁后带来的风险。

e）定量定性结合：以定性与定量相结合的方式识别重要网络数据，根据具体数据类型采取不同识别方法。某些数据，其所在行业、应用领域决定了本身的重要性；也有些数据，仅在达到一定量后属于重要网络数据，此时需要进行定量描述。

f）坚持动态识别：重要网络数据的识别工作是动态而非静态的。一方面，在重要网络数据类型、用途、共享方式等方面发生变化时，应及时更新清单。另一方面，重要网络数据的“重要性”有时效，在识别时应当确定其时效。

5 重要网络数据概述

5.1 重要网络数据特征

符合以下一个或多个特征的，是重要网络数据。

a）能直接挖掘或与其他数据关联后挖掘出国家秘密、批量个人信息。

b）关系国家关键基础设施、关键信息基础设施安全，反映安保布置情况、脆弱性、关键参数等，泄露后可能被用来实施攻击破坏等行为，如关键信息基础设施漏洞信息。

c）有军事战略价值，泄露或破坏后可能会损害国防战略安全、削弱国家军事防御能力，如满足一定精度条件的地理信息。

d）经济发展、社会运行、人民群众日常生活所依赖，属于基础数据，如天气数据、导航数据。

e）关系国家科技竞争实力，或具有重大经济价值，反映重大发明发现、知识产权成果，如大型软件源代码。

f）关系工业生产安全，泄露或破坏后可能带来巨大经济损失、人员伤亡，如一定级别的工业数据。

g）关系生物安全与生态安全，泄露或破坏后可能引发大型传染病流行、外来生物入侵、农作物病虫害等情况，或影响饮用水与食物安全、空气质量等，如病毒试验数据。

h）关系资源安全，泄露或破坏后可能影响或危害水资源、能源资源、土地资源、矿产资源、海洋资源、生物资源、海洋资源、基因资源等的保护和利用，如基因数据。

i）由政务部门收集或产生，泄露或破坏后可能被不当利用，引发政策误读等不良反应，影响宏观调控、政府职责履行，或对其他组织和个人的合法权益带来不利影响。

j）泄露或破坏后可能影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生物、生态、资源、核设施等国家安全事项的其他信息。

5.2 重要网络数据面临的安全威胁

重要网络数据面临的安全威胁包括但不限于：

a）被攻击的威胁。攻击者利用信息系统漏洞或通过植入木马、DDoS（分布式拒绝服务）等方式，入侵数据所在的系统，窃取、删除或篡改数据，影响数据保密性、完整性、可用性。

b）被非授权访问的威胁。因重要网络数据价值很大，可能被非授权人员收集、知悉、使用或传输

到境外，从而危害国家安全、公共利益。非授权访问，既有可能由外部攻击造成，也有可能表现为无合法、正当、必要理由而收集用户或其他组织数据，或者掌握重要网络数据的组织或其内部人员有意泄露或滥用重要网络数据。

c）真实性、准确性威胁。某些用于公开发布的数据，如遭到伪造、篡改，可能产生严重后果。例如，天气预报、环保监测数据等只能由权威机构发布。此类情况下，数据的完整性、发布源的真实性、发布平台的安全性、转载的一致性等均可能需要重点考虑。

d）数据汇聚、整合、分析后的安全风险。应当考虑数据汇聚、整合、分析的过程可能导致不宜公开的信息泄露的风险。但同时也应当避免以数据汇聚、整合、分析风险为由对“重要网络数据”概念泛化，可通过技术和管理机制降低数据被汇聚、整合、分析的风险。例如，强化数据隔离和访问控制机制，实现数据“可用不可见”，即原始数据不离开本地，用户只能按需访问数据处理结果。

5.3 重要网络数据类别

从数据的作用、受破坏后可能带来的影响等角度，将重要网络数据分为以下类别：

a）经济运行类。即反映国家宏观经济运行情况，或对经济运行可能产生重大影响的数据。不含国家秘密和已公开的数据。但可能通过汇聚、整合、分析而导出涉及国家秘密的原始数据、基础数据、局部数据，可能属于重要网络数据。拟公开的数据，在公开前可能属于重要网络数据。

b）人口与健康类。即能够反映自然人健康状况、生理指标、公共卫生事件、食品药品安全等的信息。

c）自然资源与环境类。即反映自然资源与环境状况、自然灾害事件、自然资源开发利用情况等的数据。除国家秘密外，其他不宜公开或尚未公开的数据属于重要网络数据。

d）科学技术类。即对国家安全、国家竞争力有潜在价值和重大影响的知识成果，以及其他具有重大经济价值、尚未公开的工艺、配方等数据。这类数据不仅包括记录科学实验结果的数据，还包括对科研成果的所有电子形式的描述与记录，包括但不限于源代码、说明文档、配方、图纸等。

e）安全保护类。即反映重点目标、重要场所安全保护情况，或可能被利用来对重点目标、重要场所实施攻击、破坏等行为的数据。包括物理类安保数据和网络类安保数据。

f）应用服务类。即各类企业或其他组织在提供服务的过程中，所收集、产生的有关数据。既包括用户委托的重要网络数据，也包括在向政府部门、公共企事业单位（包括但不限于教育、卫生健康、供水、供电、供气、供热、环境保护、公共交通等单位）用户或重点项目（如国家重大建设工程）提供服务的过程中，所产生的有关用户基本信息、使用情况等数据。如汽车生产制造企业掌握的重点用户行驶里程、轨迹等信息。

g）政务信息类。即由国家政务部门所收集或的产生的，除国家秘密外较为敏感或不宜公开的信息。

h）其他类。以上类别未包括，但也会对国家安全、经济发展以及公共利益产生重大影响的其他非国家秘密的数据。

5.4 重要网络数据主要分布

可能收集、产生、处理、存储、传输重要网络数据的实体包括但不限于：

a）政务部门。一些数据资源分布在政务部门、直属事业单位和其他相关部门中，在政务部门内部流转，或对社会开放，包括宏观经济数据、金融监管数据、人口资源数据、健康数据、执法数据（如事故调查、证人信息）、交通运输数据等。

b）重点行业企业。涉及国计民生的各重点行业，特别是关键信息基础设施运营者，在运营中可能收集、产生大量重要网络数据，如金融交易数据、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。

c）公共服务机构。如医院（拥有健康医疗数据）、高校（拥有教育数据）等，收集、产生的很多

数据属于重要网络数据。

d）具有相应资质的权威专业机构。如从事地理、地震、天文、气象等科学数据的采集、处理、汇交、保管、服务、使用的单位，收集、产生的很多数据属于重要网络数据。

e）科研机构。大量科研成果关系国家科技实力与竞争能力，某些科研成果还属于出口管制物项。此外，还有一些机构拥有的知识产权具有重大战略或经济价值，也属于重要网络数据。本标准所指的“科研机构”泛指一切可以产生科研成果或拥有知识产权，且从事研发活动的组织，包括高校、科研院所，也包括民营企业、行业组织等成立的研究机构。

f）互联网企业。企业在线提供导航、电子商务、即时通信等服务时，需要收集大量信息，同时也在产生海量信息。其中一些信息涉及经济、地理、人口、法人等国家基础数据，应当进行特别保护。

g）实体经济企业。当前绝大多数产品和服务都在线运行，至少也是在线升级，云服务成为重要趋势，导致各类产品和服务供应商可以远程实时掌握用户数据。在某些特殊应用中，这些数据可能具有重大价值。例如，大型工程施工设备生产商可以通过设备上安装的导航和无线通信模块，远程获得敏感工程的物理位置、施工土石方等数据。

6 重要网络数据识别流程

6.1 明确行业重要网络数据识别规定

行业主管监管部门明确本行业的重要网络数据识别规定。没有行业主管部门的，遵照地方网信部门规定执行。

重要网络数据识别规定主要包括但不限于以下内容：

a）本行业重要网络数据的子类、二级子类（由主管监管部门自行确定）。

b）以定性或定量方法描述的本行业重要网络数据识别依据。

c）重要网络数据报送格式。

d）本行业组织实施重要网络数据识别的工作机制。

6.2 识别和描述本组织的重要网络数据

根据主管监管部门制定的重要网络数据识别规定，各类组织识别本组织内重要网络数据，包括梳理数据资产、判断安全影响、识别重要网络数据、识别结果审核、确定并描述重要网络数据。

a）梳理数据资产：对本组织内的数据资产进行盘点、梳理与分类，形成组织数据资产清单。

b）判断安全影响：明确资产清单中各类数据的用途、面临的主要安全威胁，判断数据安全性（保密性、完整性、可用性等）遭破坏后可能对国家安全、公共利益等造成的影响。

c）识别重要网络数据：根据本行业的重要网络数据识别依据，初步判定组织数据资产中的重要网络数据。必要时，可使用自动化技术工具分析结构化数据、半结构化数据及非结构化数据，根据数据规模量级、关键字段、关联规律等识别包含的重要网络数据。

d）识别结果审核：组织对识别结果进行审核。

e）确定并描述重要网络数据：根据本标准第 7 章重要网络数据描述方法和主管监管部门提出的报送格式要求，形成本组织的重要网络数据识别结果。

6.3 报送与备案

各类组织通过主管监管部门指定的工具或途径，以在线或离线方式向主管监管部门报送本组织内的重要网络数据识别结果。

首次报送后，如重要网络数据在类型、用途、共享方式等方面发生变化，应当及时将变化情况报送主管监管部门。

注：各实体报送内容不包含数据本身。

各类组织报送的识别结果将作为行业重要网络数据目录的制定依据。行业主管部门形成本行业重要网络数据目录后，按规定向国家网信部门或其他规定的部门进行备案。

7 重要网络数据描述方法

本标准提出了如表 1 所示的重要网络数据表示方法。

a）“类别”是重要网络数据的第一级分类，共包括“经济运行类”、“人口与健康类”、“自然资源与环境类”、“科学技术类”、“安全保护类”、“应用服务类”、“政务信息类”、“其他类”等 8 类。

b）“子类”是重要网络数据的第二级分类，由重要网络数据所在的行业主管监管部门规定确定。

c）“二级子类”是重要网络数据的第三级分类，由重要网络数据所在的行业主管监管部门确定。根据具体情况，有的重要网络数据不含二级子类。

d）“标识”指重要网络数据的简称，以 3 级英文字母表示，每一级使用两个英文字母，一般是相关数据类型英文名称的首字母。第一级分类的标识分别为：经济运行类——EC；人口与健康类——HE；自然资源与环境类——NA；科技技术类——ST；安全保护类——SF；应用服务类——US；政务信息类——GO；其他类——OT。子类和二级子类的标识由行业主管监管部门确定。

e）“行业”指重要网络数据所在的具体行业。

f）“主管监管部门”指重要网络数据所在的具体行业的主管监管部门。

g）“影响”指重要网络数据对国家安全、经济运行、社会稳定、公共健康和安全的影响，即重要网络数据之所以“重要”的理由。

h）“面临的主要安全威胁”指重要网络数据在保密性、完整性、可用性、真实性等方面可能面临的安全威胁。

i）“现有管理政策”指本组织内重要网络数据的安全保护需要遵循的行业管理政策。

j）“时效”指重要网络数据维持“重要性”的时间长度。原则上，重要网络数据的时效不超过国家秘密的保密期限。时效过后，便不再属于重要网络数据。

k）“来源”指重要网络数据如何收集或产生。

l）“用途”指本组织使用重要网络数据的目的以及具体用法。

m）“共享交换情况”指本组织与组织外的其他实体共享、交换重要网络数据的情况，含数据出境情况。

n）“保护情况”指本组织对重要网络数据采取的安全保护措施。

o）“备注”用于描述其他需要说明的事项。

表 1 重要网络数据描述方法

类别	子类	二级子类	标识	行业	主管监管部门	影响	面临的主要安全威胁	适用的现有管理政策	时效	来源	用途	共享交换情况	保护情况	备注

附 录 A
（资料性）
典型重要网络数据参考示例

本标准附录从二级子类的角度提供了典型重要网络数据的参考示例，其中的子类划分仅为示例，并非实际确定的子类。重要网络数据的子类与二级子类划分遵从各行业主管监管部门发布的识别规定。

A.1 经济运行类

典型的经济运行类重要网络数据主要包括：

a）战略储备数据。战略储备是指国家为了应付战争和其他意外情况，保障国民经济正常运行和国防需求，而在平时有计划地建立的一定数量的物资、能源等方面的储存或积蓄。反映战略储备计划、储备地点、储备量等情况的数据中，除国家秘密外，其他数据属于重要网络数据。战略储备数据还可以分为粮食储备数据、物资储备数据、能源储备数据等子类。

1）粮食储备数据，涉及国家战略物资储备规划、国家储备品种目录，以及国家粮食、棉花和食糖储备量、仓储分布等情况。

2）物资储备数据，涉及战略物资生产能力、储备量、仓储分布等情况。

3）能源储备数据，如：原油、成品油、天然气的库存信息、生产信息（如生产量、主要炼厂相关信息、生产方式、销售流向等）、储备量、仓储分布、管线信息（如原油、成品油、天然气管道的输量等）；煤炭资源信息（如矿区、各煤种的储量等）、生产信息（如矿井井口坐标、开采水平标高等）。

4）其他战略物资储备数据，涉及其他战略物资生产能力、储备量、仓储分布等情况，如国家主要化工产品生产能力、储备情况、重大化工进出口项目等信息。

b）工业生产数据。作为新的生产要素资源，分布于关键信息基础设施运营者的生产系统中，主要包括：

1）工业控制数据，关键信息基础设施运营者在生产过程中倚赖的控制信息、工况状态、工艺参数等生产数据。

2）研发设计数据，重要行业工业企业研发设计数据。

3）重要装备数据，涉及生产安全保障类装备和高技术关键装备，如军事、航空航天装备等的生产制造信息，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。

4）重要领域供应链信息，涉及重要物资装备、各类电子信息设备、软件产品和信息技术服务在国防军事、政务和公共服务等重要领域中的销售、使用、运行、维护等信息，如：购买方名单、交易价格、交易数量、采购周期、采购产品型号、应用领域、产品去向、建设方案、更换/升级频率、运行日志、维护服务信息等；国防军工相关单位采购品种、型号、数量、途径、代理商等信息；电子信息产品在重要行业的运行、保养和维修等使用信息。

c）金融数据，在金融业务活动中产生，含有用户账户等信息，或反映金融交易情况的数据，如金融机构、非银行支付机构以及为上述机构提供清算服务的特许清算机构在经营过程中收集或产生的数据。

d）中央企业商业秘密，指不为公众所知悉、能为中央企业带来经济利益、具有实用性并经中央企业采取保密措施的经营信息和技术信息，如：重点企业生产规模、产量等产业实力或潜力相关信息；军工企业采购品种、数量等重要销售信息；军工科研生产单位内部名称、地理位置、建设计划、安防规划、保密等级、警卫保护、厂房图纸、库房容积、储备情况等信息。

e）统计数据，该类数据反映国民经济运行总体情况，影响国家宏观调控能力。

1）在统计结果公布前，除国家秘密以外的数据属于重要网络数据，包括：经济运行数据；产业发展数据；产业运行数据，如规模以上重点产业企业数量、产值、销售收入、利润等基本情况，产业新在建项目数量、项目可行性报告、投资额、资金来源等情况，及重点产业产品进出口贸易情况；与国家安全和社会公众利益密切相关的电信和互联网统计分析数据等。

2）统计结果公布前后，统计调查中获取的原始数据属于重要网络数据，统计调查对象的商业秘密或者在统计调查中获得的能够识别或者推断单个统计调查对象身份资料的数据属于重要网络数据。

A.2 人口与健康类

典型的人口与健康类重要网络数据主要包括：

a）人口数据，涉及人口普查、基因数据、遗传资源等，如：人口普查资料、生命登记信息、人类遗传资源信息、基因测序原始数据、人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料的情况。

b）健康医疗数据，如：

1）诊疗与健康管理信息，涉及电子病历、检测结果、健康档案等各类诊疗、健康数据信息，以及健康医疗数据开发利用结果等信息。

2）疫情管理相关信息,涉及突发公共卫生事件与传染病疫情监测过程中获得的疫病流行情况，疫情防控过程中获得的病源跟踪、物资调配、交通运输等相关信息。

c）食品药品数据，如：

1）药品数据，涉及国家战略安全的药品在药品审批过程中提交的药品实验数据，如：在药品不良反应报告和监测过程中获取的患者和报告者信息；在动物模型上进行的药理、毒理、稳定性、药代动力学等试验数据，在人体中进行的临床试验数据，以及与药品的生产流程、生产设施有关的试验数据。

2）医疗器械实验数据，涉及《医疗器械分类规则》所定义的第二类、第三类医疗器械临床试验数据/报告。

3）食品安全相关信息，涉及食品安全溯源标识信息，包括产品名称、执行标准。药品溯源标识信息，包括追溯编码、产品名称、执行标准、配料、生产工艺、标签标识；

4）食品药品安全重大（紧急）事件信息。

A.3 自然资源与环境类

典型的自然资源与环境类重要网络数据主要包括：

a）地理数据，可包括：

1）地图数据，涉及除涉密信息之外的所有地图数据。

2）导航数据，涉及属于《关于规范卫星导航定位基准站数据密级划分和管理的通知》中所列的非涉密受控基准站数据；提供 LBS 过程中产生的用户位置数据集；北斗导航系统建设运行数据，如灾备、服务能力等数据；导航服务衍生应用中记录的未公开场所的位置数据；北斗导航用户名录、属性、装备识别号及短信息服务内容等数据；地理信息坐标轨迹及含位置信息的车辆移动数据。

3）特殊测绘数据，涉及《测绘管理工作国家秘密范围的规定》规定的涉密信息以外的国家重力控制点成果、加密重力测量成果、航空重力测量成果、海洋重力测量成果、全国性重力异常成果；军事禁区的磁力测量数据和我国海域磁力测量数据及其衍生品；境内优于 25 米网络的数字高程模型、数字地表模型数据。

4）重点目标地理信息，涉及标注重点目标属性的地理信息，如：标注国家或地区重要安全警卫目标、设施和关键基础设施信息的遥感影像；国家或地区重要安全警卫目标、设施的带有位置精度信息的实景影像；国家版图的重要特征点，地势、地貌分区位置，以及国务院测绘地理信息主管部门商军地有关部门确定的其它重要自然和人文地理实体的位置、高程、深度、面积、长度等地理信息；能源、金属、非金属等主要矿物的地理分布情况及开采储量、设计储量、远景储量等储量信息，尤其是与国家安全密切相关的矿产情况；大型水利设施、电力设施、通信设施、石油和天燃气设施、燃气设施、炼油设施、重要战略物资储备库、气象台站、降雨雷达站和水文观测站（网）等涉及国家经济命脉，对人民生产、生活有重大影响的民用设施地理信息；监狱、看守所、拘留所、强制隔离戒毒所等与公共安全相关的单位地理信息；公开机场的内部结构及运输能力属性；渡口的内部结构及属性等。

5）未公开的重点目标的地理信息，如：专用铁路及专用铁路站内火车线路、铁路编组站，未公开的专用公路；未公开的机场（含民用、军民合用机场）和机关、单位的信息。

b）水利数据，主要包括：

1）水情信息，涉及未经批准发布的水、旱情预报信息；

2）水利工程信息，涉及大型水利设施及水利工程建设运行管理资料。

3）水文观测数据，涉及未公开的水文分析结果；七大江河流域及重要地区水的中长期供求计划；全国江河湖泊水文观测数据等。

c）地震数据，主要包括：

1）地震预报信息，涉及地震预测结果及基础数据等。

2）地震灾害信息，涉及地震发生、灾害状况等。

d）气象数据，主要包括：

1）气象观测数据，如未公开广播的我国气象卫星原始资料；为国家保密任务或者军事部门保密任务专门设置的气象台站观测气象数据、特定管制范围内的各种气象数据，以及专门统计整编和分析的重要气象数据。

2）专项专业气象数据，如为作战、军事演习和训练、国防科研实验等任务专门提供的气象数据；为高科技或者特殊科学试验研究获得的气象和空间大气监测数据；通过非国际交换途径获得的各种国外气象数据；海洋气象、空间天气、历史气候代用数据、气象灾害数据、航空气象数据、交通气象数据、科学试验考察数据及相应元数据。

3）未公布的气象预报数据，如我国未参加国际交换的地面气象、高空气象、气象辐射、大气成分观测数据和统计整编数据、气象雷达基数据及相应元数据，我国未公布的数值预报产品。

e）环保数据，主要包括：

1）环保监测数据，涉及未公布的长时间系列环保监测数据以及重大污染事故情况，如：未公布的长时间系列各行业环境污染的重要污染源监测数据和危害程度以及重大污染事故情况；未公布的长时间系列大、中城市供水水源的水质资料及主要江湖、河段水质监测资料及监测系统信息；未公布的长时间系列城市空气质量监测资料及相应监测系统信息；未公布的土壤污染监测或调查数据；未公布的放射性污染监测信息、未公布的核与辐射应急监测信息。

2）环境影响数据，如采煤沉陷区面积、环境损害程度、矿井水外排量等。

f）海洋数据，主要包括海洋环境监测数据，如：

1）涉及海底地形、海洋水文、海洋气象、水声环境和海洋物理场等观测和统计整编数据；

2）涉及领海内的温盐、水声、底质、潮汐、海流实测数据和相关成果；

3）涉及未公布的海洋生态环境监测数据。

A.4 科学技术类

典型的科学技术类重要网络数据主要包括：

a）出口管制物项，涉及针对列入国家出口管制清单的物项，描述这些物项的设计原理、工艺流程、制作方法的信息以及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告。

b）知识产权，涉及针对与国防、国家安全相关的非涉密知识产权，以及具有重大经济价值的、未公开的智力成果，描述这些成果具体内容的信息属重要网络数据。

c）重大发明发现，如在科学研究、产业实践过程中产生的，具有重大战略意义或经济价值的论文、报告、实验数据等。

d）国家科技计划，包括：

1）与国家安全直接密切相关的国家科技计划（含国家重大专项、重点研发计划）项目在规划和实施过程中产生可能涉及国家安全和重大经济社会利益的重要网络数据，如可行性研究报告、建设方案、科学数据、尚未公开的科技报告；

2）国家科技计划管理过程中收集、产生的可能影响国家安全、社会公共利益的信息，如信息系统记录的用户行为日志等；

3）可真实、准确反映国家科技、国民经济等各种情况的国家大型科学仪器活动信息；

4）工业科技发展重点任务中与安全相关的关键科技内容等。

A.5 安全保护类

典型的安全保护类重要网络数据主要包括：

a）物理安全数据。可被犯罪分子、恐怖分子利用，对物理目标或以物理手段发动攻击，危害国家安全、公共安全和公民生命安全。包括：

1）重要场所与目标数据，如重点安保单位、重要生产企业、国家重要资产（如铁路、输油管道）、人群聚集场所的施工图、内部结构等情况；民用核设施安全和运行相关信息。

2）安保装备数据，涉及安保装备设计原理、使用方法、性能指标、破解方法等。

3）安保部署数据，涉及敏感场所、国家重大活动等的安保部署，包括人员部署情况、设备部署情况、应急预案等。

4）危化品数据，涉及危化品制作工艺、危化品储备地点、危化品运输、危化品安全影响信息等，如：重要地区化工建设、计划以及军用化学品出口信息；生产、储存危险化学品的单位，其作业场所的通信设置、报警装置、警卫保护措施等相关信息；企业生产和储存的剧毒化学品、易制爆危险化学品的数量、流向；剧毒化学品和易爆危险化学品的道路运输、水路运输、航空运输等相关信息。

5）音视频信息，涉及超过 500 个摄像头采集的视频数据，或超出 1 万人的音频数据。

b）网络安全数据，可被网络攻击者或恶意竞争者利用，以攻击网络系统或通过网络发起攻击的数据，包括：

1）关键信息基础设施网络安全防护信息，涉及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。以电力系统为例，包括电力各系统配置信息，如配电自动化系统、生产管理系统、高级量测体系、电能质量监控系统、用户能效管理系统等，电力监控系统安全防护方案、网络与信息系统安全防护方案，以及电力专用加密算法、核心芯片设计等。

2）关键信息基础设施规划建设信息，涉及关键信息基础设施规划及建设环节产生的敏感数据，包括整体规划设计、核心系统建设方案、主要网络拓扑结构图等。以电信和互联网为例，

可包括固定通信网省际长途网、IP 承载网、全国 IP 骨干网的规划设计方案、网络拓扑结构图。

3）关键信息基础设施运行维护数据，涉及关键信息基础设施运行维护过程中产生和收集的敏感数据以及运行日志、事件处置情况等，如：系统实时运行信息和实时状态监控信息；核心设备及基础软件版本号和配置信息、主要系统内网 IP 地址分配信息、网络及系统运行重要维护日志等。

4）漏洞与重大事件信息，如：未公开的漏洞；关键信息基础设施网络安全监测报告、评估报告等；重要网络安全预警监测信息、安全审计记录、按照行业主管部门要求采集并记录的网络与信息安全相关监测处置数据、灾备信息等。

5）应急通信数据，如应急通信系统规划、建设、运行相关信息，应急通信事件分级信息和应急预案，重大活动行动方案、保障预案信息、应急通信装备物资储备、保障队伍部署等.

6）网络安全厂商客户信息，如关键信息基础设施客户与具体产品、服务的对应关系。

7）网络安全重大发现与重要研究成果等，如新的攻击方法、新的算法、颠覆性网络安全防御技术等。

8）无线电数据，如：国家重要行业如交通运输、渔业、海洋系统、航空、航天、军事、广播电视等行业使用的涉及国家主权、安全的无线电频率和台站信息；开展重大活动保障及国家安全类的无线电监测工作时涉及的重要信息，包括无线电监测站的核心功能和参数指标信息，以及重要、敏感频率的监测信息样本，重要、敏感频段的频段扫描数据和时间占用度等电磁环境信息。上述信息中已纳入国际电信联盟（ITU）国际频率登记总表（Master International Frequency Register，MIFR）内的信息除外；国家无线电管理机构正在向或需向 ITU 进行申报的无线电网络数据除外。

A.6 应用服务类

典型的应用服务类重要网络数据主要包括：

a）用户委托数据。在向用户提供服务的过程中，用户的重要网络数据转移到企业或其他组织的信息系统之中，仍属于重要网络数据。

b）用户使用数据，涉及在向政府部门、公共企事业单位（包括但不限于教育、卫生健康、供水、供电、供气、供热、环境保护、公共交通等单位）用户或重点项目（如国家重大建设工程）提供服务的过程中，所产生的有关用户基本信息、使用情况等数据，如：全国直播卫星用户信息，汽车生产制造企业掌握的用户行驶里程、轨迹等信息，互联网服务单位收集、使用、提供的用户位置信息，批量的电子商务交易记录、个人消费信息、企业和个体商家经营数据、信用记录、信用评价和服务信息，以及对上述数据进行加工形成的可能影响国家安全的相关信息等。

A.7 政务信息类

典型的政务信息类重要网络数据主要包括：

a）执法相关数据。如案件类信息、执法对象类信息、执法手段类信息等。

b）政府政策与决策文件，包括：

1）政策法规支撑性材料，涉及尚未公开的政策文件，支撑政策法规起草的调研、统计数据等资料，如与国家安全和重大经济社会利益直接密切相关的国家重大政策措施、重点任务、关键内容、主要技术资料等。

2）政策规划和实施资料，如政策规划和实施过程中收集和产生的可能影响国家安全、社会公共利益的信息；产业发展规划、发展重点、近期国家级和部重点研发支持项目等。

3）其他内部文件或不宜公开的资料，涉及标有“内部”或含有不宜公开的内容等。

c）公民企业类数据。如公民或企业的上报信息、涉及公民或企业的监管决定等数据。

d）其他敏感政务信息，涉及其他不宜公开的政务信息。

参考文献

[1] NIST SP 800-60《将各类信息与信息系统映射到安全类的指南》

[2] NIST SP 800-171《保护非联邦系统和机构的受控非密信息》（2016年12月发布，2018年2月更新第一版，2019年6月至8月第二版草案征求意见）

[3] NIST SP 800-171A《受控非密信息安全要求评估》（2018年6月发布）

[4] NIST SP 800-171B《保护非联邦系统和组织中的受控非密信息：关键程序和高价值资产的增强安全要求》（2019年6月发布草案）

[5] 国家互联网信息办公室《数据安全管理办法（征求意见稿）》(2019年5月发布)

[6] 国务院办公厅关于印发科学数据管理办法的通知（国办发〔2018〕17号）

[7] 教育部机关及直属事业单位教育数据管理办法（教发厅〔2018〕1号）

[8] 国土资源数据管理暂行办法（国土资发〔2010〕142号）

[9] 国家健康医疗大数据标准、安全和服务管理办法（试行）（国卫规划发〔2018〕23号）