附件：

ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXX—XXXX

信息安全技术 数据出境安全评估指南

Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment

（草案）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
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：

引　言

近年来，随着互联网的蓬勃发展，数据流动无处不在。数据流动所产生的经济价值和社会价值凸显，这一过程中的安全风险也随之增加，国家安全、社会公共利益、个人隐私受到严重威胁，防范数据泄露和滥用所产生的风险日益紧迫。

本标准规定了数据出境安全评估流程、评估要点、评估方法等内容，网络运营者按照本指南对其向境外提供的个人信息和重要数据进行安全评估，发现存在的安全问题和风险，及时采取措施，防止个人信息未经用户同意向境外提供，损害个人信息主体合法利益，防止国家重要数据未经安全评估和相应主管部门批准存储在境外，给国家安全造成不利影响。

信息安全技术 数据出境安全评估指南

1 范围

本标准对个人信息和重要数据出境安全评估的工作要求、方法流程、评估内容和结果判定进行了规范。

本标准适用于网络运营者开展的个人信息和重要数据出境安全评估工作，也适用于行业主管或监管部门对网络运营者开展个人信息和重要数据出境安全评估进行的指导、监督等工作。

网信部门、行业主管或监管部门依职权开展的个人信息和重要数据出境安全评估，可参考本标准。

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 25069-2010 《信息安全技术 术语》

GB/T AAAA 《信息安全技术 个人信息安全规范》

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络运营者 network operator

本标准所指网络运营者，是指网络的所有者、管理者和网络服务提供者。

3.2

数据 data

本标准中所称数据是网络运营者在中华人民共和国境内运营中收集和产生的电子形式的个人信息和重要数据。

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与其他信息结合识别自然人个人身份或者反映特定自然人活动情况的各种信息，包括但不限于自然人的姓名、出生日期、身份证号码、通信通讯联系方式、个人生物识别信息、住址、账号密码、财产状况、位置和行为信息等。

3.4

个人敏感信息 sensitive personal information

一旦泄露、非法提供或滥用可能危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等的个人信息。

3.5

重要数据 important data

与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照附录A。

3.6

数据出境 data cross-boder transfer

将在中华人民共和国境内收集和产生的电子形式的个人信息和重要数据，提供给境外机构、组织、个人的一次性活动或连续性活动。

注：境外数据经由中华人民共和国中转，未经任何变动或加工处理的情形不属于数据出境。

3.7

数据出境安全风险 risk of data cross-borders transfer

数据出境及再转移后被泄露、毁损、篡改、滥用等可能对国家安全、社会公共利益、个人合法利益带来的风险。

3.8

提供 provide

网络运营者主动向境外机构、组织或个人提供数据，或通过其他途径发布数据的行为，包括其用户使用网络运营者提供的产品或服务的功能，向境外机构、组织或个人提供数据的行为。

注：网络运营者提供已经被依法公开披露的数据除外。

3.9

自评估 self assessment

网络运营者依照国家法律法规和有关标准的规定，对数据出境组织开展安全评估活动。

3.10

数据脱敏处理 data desensitization

网络运营者对某些敏感数据通过脱敏规则进行数据变形处理，实现对敏感隐私数据的可靠保护。

3.11

数据保护能力 data protection capability

网络运营者在数据的存储、处理、传输过程中确保数据安全的能力。

4 评估流程

4.1 自评估启动

网络运营者应在如下情况启动自评估：

a）产品或服务涉及向境外机构、组织或个人提供数据的；

b）已完成数据出境安全评估的产品或业务所涉及的数据出境，在目的、范围、类型、数量等方面发生较大变化、数据接收方变更或发生重大安全事件的。

4.2 制定数据出境计划

网络运营者应首先制定数据出境计划，计划的内容包括但不限于：

a） 数据出境目的、范围、类型、规模；

b） 涉及的信息系统；

c） 中转国家和地区（如存在）；

d） 数据接收方及其所在的国家或地区的基本情况；

e） 安全控制措施等。

4.3 评估数据出境计划的合法正当和风险可控

数据出境安全评估首先评估数据出境计划的合法性和正当性；数据出境活动不具有合法性和正当性，不得出境。在此基础上再评估数据出境计划是否风险可控，有效避免数据出境及再转移后被泄露、损毁、篡改、滥用等风险。具体流程如图 1。

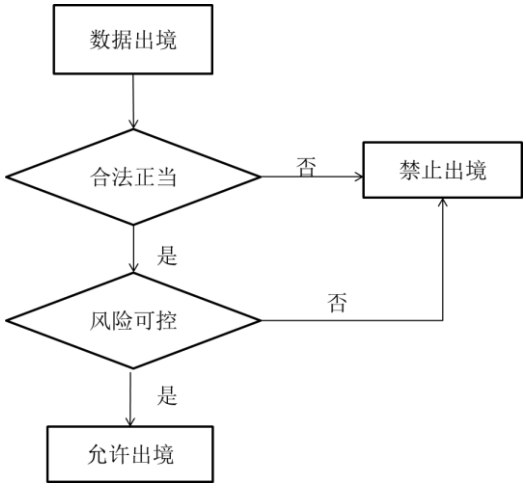

图 1 数据出境安全评估原理

4.4 评估要点及方法

网络运营者需按照本标准第 5 章中的评估要点进行自评估，评估方法参考附录 B；经评估，出境安全风险为极高或高的，个人信息和重要数据不得出境。

4.5 评估报告

网络运营者在完成对数据出境计划的评估后，应形成评估报告，评估报告应至少保存5年。

4.6 检查修正

如数据出境计划不满足合法正当要求，或经评估后不满足风险可控的要求，网络运营者可修正数据出境计划，或采用相关措施降低数据出境风险，并重新开展自评估。

注：可用于降低数据出境安全风险的措施包括但不限于：精简出境数据内容、使用技术措施处理数据降低敏感程度、提升数据发送方安全保障能力、限定数据接收方的处理活动、更换数据保护水平更高的接收方、选择政治法律环境保障能力较高地区的数据接收方等。在进行相应调整后，可重新对数据出境进行安全风险评估。

5 评估要点

5.1 合法正当

数据出境计划应同时满足合法性和正当性的要求：

a) 合法性包括：
   1） 不属于法律法规明令禁止的；
   2） 符合我国政府与其他国家、地区签署的关于数据出境条约、协议的；
   3） 个人信息主体已授权同意的，危及公民生命财产安全的紧急情况除外；
   4） 不属于国家网信部门、公安部门、安全部门等有关部门依法认定不能出境的。
b) 正当性包括：
   1） 网络运营者在合法的经营范围内从事正常业务活动所必需的；
   2） 履行合同义务所必需的；
   3） 履行我国法律义务要求的；

4）司法协助需要的；

5）其他维护网络空间主权和国家安全、社会公共利益、保护公民合法利益需要的。

5.2 风险可控

5.2.1 概述

评估数据出境计划的风险可控，应综合考虑出境数据的属性和数据出境发生安全事件的可能性：

a） 数据属性：

1）个人信息的属性，包括数量、范围、类型、敏感程度和技术处理情况等；

2）重要数据的属性，包括数量、范围、类型和技术处理情况等。

b） 数据出境发生安全事件的可能性:

1）发送方数据出境的技术和管理能力；

2）数据接收方的安全保护能力、采取的措施；

3）数据接收方所在国家或区域的政治法律环境。

5.2.2 个人信息属性评估要点

5.2.2.1 类型和敏感程度

应识别个人信息中所包含的信息类型，并判断其涉及的个人敏感信息的数量。

5.2.2.2 数量

应评估所涉及的个人信息主体数量以及所涉及的主要人群的群体特征，当数据出境涉及的个人信息主体数量达到或超过一定量级，或涉及某一特定群体时，个人信息会出现数据汇集后的衍生价值。

5.2.2.3 范围

应评估出境个人信息范围是否符合最小化原则：

a） 向境外传输的个人信息应与出境目的相关的业务功能有直接关联。直接关联是指没有该信息的参与，相应功能无法实现；

b） 向境外自动传输的个人信息频率应是与数据出境目的相关的业务功能所必需的最低频率；

c） 向境外传输的个人信息数量应是与数据出境目的相关的业务功能所必需的最低数量。

5.2.2.4 技术处理情况

应对个人信息技术处理情况进行评估，具体包括：

a） 是否使用技术措施对个人信息进行了脱敏处理；

b） 脱敏效果是否有效可靠，达到了合理程度的不可逆。

5.2.3 重要数据属性评估要点

5.2.3.1 类型

应评估重要数据类型，评估是否包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据、关键信息基础设施的系统漏洞、安全防护等网络安全信息等出境后出现泄露或滥用等情形，将对国家安全和社会公共利益产生严重的影响的重要数据。

5.2.3.2 数量

应评估重要数据出境数量，重要数据数量响其所蕴含的社会、经济价值，数量越大，发生泄漏、披露或滥用时，造成的国家安全危害和社会公共利益风险越大。

5.2.3.3 范围

重要数据范围应符合最小化原则：

a) 向境外传输的数据应与出境目的相关的业务功能有直接关联。直接关联是指没有该信息的参与，相应功能无法实现；
b) 向境外自动传输的数据频率应是与数据出境目的相关的业务功能所必需的最低频率；
c) 向境外传输的数据数量应是与数据出境目的相关的业务功能所必需的最低数量。

5.2.3.4 技术处理情况

应对重要数据技术处理情况进行评估，具体包括：

a) 是否使用技术措施对重要数据进行了脱敏处理；
b) 脱敏效果是否有效可靠，达到了合理程度的不可逆。

5.2.4 发送方数据出境的技术和管理能力

5.2.4.1 管理制度保障能力

a) 安全管理制度：
   1) 具备数据出境安全管理体系，包括安全策略、管理制度、出境操作流程等；
   2) 安全策略管理文件中包含总体目标、重要数据的范围、出境原则、出境安全总体框架等；
   3) 各项数据出境安全管理制度中，应该覆盖数据的数量、范围、类型及其敏感程度的等内容；
   4) 对个人信息应体现分级的数据出境安全操作流程，包括出境流程、后续安全保障等；
   5) 对重要数据实施严格的出境安全操作流程，包括出境流程、后续安全保障等。
b) 人员管理机制：
   1) 指定专职人员，应在组织内部指定专门的数据出境安全管理人员，并确保其履行相应职责，包括但不限于：数据出境转移的审计、合规管理、评估报告的编写与提交、配合主管部门监督检查、处理有关纠纷等；
   2) 建立人员培训机制，应在组织内部建立人员培训机制，确保被培训人员达到培训要求，可以进行数据出境转移相关工作。
c) 与数据接收方签订合同，内容应包括：
   1) 建立数据安全审计机制，制定审计要求，按照审计要求开展审计工作；
   2) 配合网络运营者或个人信息主体对数据出境活动进行合理调查；
   3) 除法律规定外，在未获得网络运营者的授权以及个人信息主体知晓并同意前提下，数据接收方不得对数据进行处理、披露及再转移；
   4) 采用适当的技术安全措施以保障数据的保密性和完整性。
d) 审计机制：
   1) 对数据出境保护策略和规程、处理、安全保护措施的有效性进行审计，并形成审计结果，审计结果应能支持事件的处置、应急响应和事后调查；
   2) 审计时应采用安全措施，防止非授权访问、篡改或删除。
e) 应急预案：
   1) 当数据出境可能对数据主体权益产生危害时，应立即终止数据出境传输，并立即启动应急预案机制，采取相关措施保护数据主体的权益；
   2) 应立即将对数据主体权益产生威胁的行为、原因以及紧急处置措施等相关信息上报给数据监管机构；
   3) 在数据监管机构判定紧急处置不合理或不必要时，网络运营者应立即按要求进行更正。
f) 投诉与处置策略：
   1) 确保相关数据主体均可通过该机制对数据出境转移过程中的行为进行申诉；
   2) 指定具有相应权限的独立人员负责处理所有数据主体提出的申诉；
   3) 数据出境投诉受理及处理机制的流程等信息需向所有数据主体公开。
g) 安全事件上报机制：

1） 上报触发条件，包括发生数据泄露、数据遗失、数据接收方违约进行数据处理，以及一切可能危害国家安全、损害公共利益、违反法律或侵害数据主体权益的行为；
2） 上报内容，包括发生紧急情况的时间、数据类型、规模、内容等。

5.2.4.2 技术手段保障能力

a） 总体安全防护技术手段
1） 建立完善的数据传输保护措施；
2） 在安全边界采用防护手段并进行定期安全评估和审核；
3） 及时发现并修补安全措施存在的漏洞；
4） 具备账户权限管理技术，杜绝数据的非授权访问。
b） 数据出境日志留存，应预先建立数据出境日志留存机制，留存信息包括但不限于：审计报告、数据出境转移日志、数据被访问日志等。

5.2.5 数据接收方的安全保护能力

5.2.5.1 主体审查

a） 应具有合法资质，如营业执照、组织机构代码证、税务登记证等；
b） 经营范围应与接收数据的类型、内容相一致；
c） 无重大违法记录，包括大规模个人信息泄露事件及违规使用个人信息的记录等；
d） 针对重要数据，应对数据接收方的背景关系进行评估。

5.2.5.2 管理保障能力

a）组织建设：
1） 应建立清晰的数据安全职能架构并定义数据安全职责；
2） 应设置专职的数据安全合规团队，识别在数据接收阶段应符合的安全合规需求；
3） 应制定数据安全职能工作规范，明确各职能岗位之间的协作关系，明确各职能岗位的运行配合机制。
b）制度流程：
1） 应依据业务需求和合规性要求，制定并执行数据安全管理的顶层方针、策略；
2） 应建立数据接收、存储、使用、传输、销毁的安全管理制度，提出各阶段的安全管理要求，并建立合理的机制保证制度的制定、发布、修订工作开展的规范性；
3） 应建立数据安全风险的防范、预警、应急处理、问责机制等；
4） 应建立数据安全管理识别流程，对数据应得到的安全保障要求进行识别，并落实相关要求到已有的数据安全控制中。
c）人员能力：
1） 组织内员工应具备良好的数据安全意识；
2） 数据安全岗位的人员应并具备专业数据安全能力；
3） 数据接收的整体负责人员应能理解并执行数据安全合规要求。

5.2.5.3 技术保障能力

a） 安全技术能力：
1） 应具备针对数据安全风险的预防、检测及响应能力；
2） 应具备保障所接收数据的保密性、完整性、一致性、可用性、可追溯性、真实性等能力；
3） 应具备整体的数据安全技术防护及应急保障体系；
4） 应具备对数据访问的身份及权限管理的能力；
5） 应具备对数据接收的数据源进行鉴别及记录的能力；
6） 应具备对数据存储介质的安全管理的能力；
7） 应具备对数据接收、存储、使用、传输、销毁等各阶段进行监控与审计的能力。

b) 信息系统：
   1）信息系统的规划、建设、部署和运维应符合所在国家或区域的信息系统安全要求；
   2）信息系统应具备保障数据安全的能力，包括身份及权限管理、风险管理、应急管理、备份恢复、日志管理等。
c) 自动化工具：
   1）应具备利用技术工具对数据安全工作的自动化支持能力；
   2）应具备对数据接收、存储、使用、传输、销毁等各阶段监控与审计的自动化工具；
   3）应建立用于数据备份和恢复的统一技术工具；
   4）应具备保障网络安全的技术工具，在网络关键节点处检测和限制从内部或外部发起的DDOS、网络攻击、数据爬虫等异常行为。

5.2.6 数据接收方所在国家或区域的政治法律环境

5.2.6.1 个人信息

只涉及个人信息出境时，对数据接收方所在国家或地区的政治法律环境的评估应包括：
a) 该国家或地区现行的个人信息保护法律、法规、标准情况，与我国个人信息保护法律、法规、标准提供的保护水平相比较的差异性；
b) 该国家或地区加入的区域或全球性的个人信息保护方面的机制，以及所做出的具有约束力的承诺；
c) 该国家或地区落实个人信息保护的机制，如是否具有法定的个人信息保护机构、相关司法机制、行业自律协会和自律机制等，以及为个人提供的行政和司法救济渠道的有效性。

5.2.6.2 重要数据

涉及重要数据出境时，对数据接收方所在国家或地区的政治法律环境评估包括：
a) 标准 5.2.6.1 的评估内容；
b) 该国家或地区在数据安全方面现行的法律、法规、标准情况；
c) 该国家或地区落实数据安全的机制，如网络安全或数据安全方面的主管机构、相关司法机制、行业自律协会和自律机制等；
d) 该国家或地区政府，包括执法、国防、国家安全等部门调取数据的法律权力；
e) 该国家或地区与其他国家或地区之间有关数据流通、共享等方面的双边或多边协定，包括在执法、监管等方面数据流通、共享的双多边协定。

附 录 A
（规范性目录）
重要数据识别指

指南中的重要数据是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：

（一）危害国家安全、国防利益，破坏国际关系；

（二）损害国家财产、社会公共利益和个人合法利益；

（三）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

（四）影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；

（五）干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

（六）危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；

（七）影响或危害国家经济秩序和金融安全；

（八）可分析出国家秘密或敏感信息；

（九）影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。

根据上述定义和行业（领域）主管部门相关规定，指南提出了各行业(领域)重要数据的范围。请各行业（领域）主管部门结合实际，明确本行业（领域）重要数据定义、范围或判定依据；并根据行业（领域）发展变化，及时更新或替换本指南中相关内容。

本指南不影响中国在《世贸组织协定》等国际协定项下义务的执行。

A.1. 石油天然气

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

a) 价值类，包括表示资源金额等信息；
b) 生产量类，包括各类生产量等信息；
c) 销售量类，包括各类销售量等信息；
d) 施工作业量类，包括各类施工作业量等信息；
e) 安全与环保类，包括计量管理、节能管理、劳保用品、危险作业区、质量控制等信息；
f) 储备类，包括储备数量、储备设施位置、坐标等信息。

A.2. 煤炭

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

a) 行业基本情况，主要包括企业数量、企业分布、企业类型、从业人员数量、从业人员分布等；
b) 行业经济情况，主要包括行业的资产、负债、收入、利润、主要经济指标、行业资金紧张程度等；
c) 行业采购情况，主要包括原材料的采购量、采购金额、采购价格以及采购周期等；
d) 行业生产情况，主要包括行业的产值、生产投入、劳动生产率、产能以及产能影响因素等；
e) 行业销售情况，主要包括行业市场规模、销售投入、人均销售水平、主要产品销售价格等；
f) 行业投资情况，主要包括行业新建项目数量、投资额、资金来源等。

A.3. 石化

主管部门：能源局。

重要数据包括但不限于：

a) 国家石油、石化工业年度和中、长期发展规划的主要经济技术指标和重大政策措施；
b) 石化工业重要生产物资年度进口计划和未分配的控制外汇金额。

A.4.电力

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

A.4.1 发电厂相关信息

a) 火电厂的用煤量、水电厂的耗水量等信息；
b) 发电机组数据，包括火电、水电等发电机组可靠性指标数据等信息；
c) 电厂内变电站的开关数据，包括厂站名、开关类型、电抗值、母线电压、投入时间、退出时间等信息。

A.4.2 输配电信息

a) 实际负荷、预测负荷等信息；
b) 输变电设备可靠性指标，包括电压等级、统计百台年数、故障率、故障次数、故障停运时间、修复时间、计检率、计检平均时间等信息；
c) 输电线路信息，包括线路段号、侧地名、侧开关号、并联号、侧省名、调度权、线路长度、导线型号、地线型号、安全电流、控制电流、导线排列、正序电阻等；
d) 线损消耗、影响线路状态的环境信息等。

A.4.3 建设运维信息

a) 装机容量、发电量、供应量等信息；
b) 同比环比增减量等信息；
c) 电力各系统配置信息，包括配电自动化系统、生产管理系统、停电管理系统、高级量测体系、电能质量监控系统、用户能效管理系统等；
d) 电力各系统运行信息，包括电压、电流、频率、波形等；
e) 电力系统实时状态监控、电力系统巡检、电力调度等信息；
f) 可靠性统计分析信息，包括可用系数、强迫停运率、平均无故障可用小时、故障率、修复率等。

A.4.4 其他信息

a) 电力各系统资产、配套安防系统相关信息；
b) 未发布的电网/电厂规划图等；
c) 城市电网管线分布图文资料；
d) 电网地理坐标信息；
e) 能够有助于入侵攻击电力基础设施的其他信息。

A.5.通信

主管部门：工业和信息化部。

重要数据包括但不限于：

A.5.1 规划建设类数据

主要包括电信网和互联网网络及信息系统在规划及建设环节产生的重要数据，如规划设计及建设方案、灾难备份系统设计及建设方案、设备地理位置、网络拓扑结构、线路路由走向、设备资产采购清单等。

A.5.2 运行维护类数据

主要包括网络及信息系统运维过程中产生、收集的重要数据，如设备及软件配置信息、IP地址分配信息及内外网转换信息、网络流量流向信息、网络及系统运行状态信息、网络及系统运行维护日志、以及系统用户资料信息等。

A.5.3 安全保障类数据

a) 网络与信息安全管理数据，如网络安全预警监测信息、系统及数据访问操作日志、安全审计记录、网络安全应急预案、违法有害信息监测处置相关数据、用户访问互联网日志数据、用户计费数据和上网记录等个人通信数据；
b) 应急通信数据，如应急通信系统规划、建设、运行相关信息等；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。

A.5.4 无线电数据

a) 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；
b) 卫星通信信息主要是指使用卫星进行通信所涉及的相关信息，主要包括卫星地面站基建、卫星地面站灾备、卫星通信用户等信息；
c) 蜂窝移动通信基站位置、蜂窝移动通信基站基建、蜂窝移动通信基站灾备、蜂窝移动通信基站收发能力等信息；
d) 无线电监测信息主要指开展无线电监测工作所涉及的相关信息，主要包括无线电监测站地理位置、天线配置、设备能力等监测设施信息，以及监测信号样本、频段扫描数据、频率时间占用度等电磁环境信息；
e) 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.5.5 统计分析类数据

主要包括：根据网络及信息系统运行、用户网络行为等过程中直接产生、收集的重要数据，以及统计分析得到的数据，如行业和企业运行情况、用户网络行为习惯分析信息、行业或业务发展预测信息等。

A.5.6 其他通信数据

a) 关键基础设施网络威胁原数据；
b) 通信内容、信令、记录等数据；
c) 基础核心技术、核心设备主要性能参数、网络信息安全整体防护能力。

A.6.电子信息

主管部门：工业和信息化部。
重要数据包括但不限于：

a) 产业运行数据，主要包括：尚未公开的规模以上电子信息产业企业数量、产值、销售收入、利润等基本情况，尚未公开的产业新在建项目数量、项目可行性报告、投资额、资金来源等投资情况，及尚未公开的电子信息产品进出口贸易情况；
b) 产业发展数据，主要包括：尚未公开的产业发展规划、发展重点、近期国家级和部重点的研发支持项目等；
c) 电子信息百强企业业务数据，主要包括：尚未公开的企业业务发展决策、投融资决策，及企业产值、销售收入、利润、研发投入、研发人员数量等内容；
d) 电子信息产品基础硬件的型号、重要参数、源代码和目标、技术方案、实验数据、检测报告、重要工艺技术等全部技术资料；
e) 国防军事领域、政务领域和公共服务领域等在关键领域或重要行业中各类电子信息设备的销售信息和使用信息，例如购买方名单、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、更换频率等；
f) 在关键领域或重要行业中电子信息产品在使用过程中的运行、保养和维修信息，例如使用信号波段、频率等设备运行参数，设备故障频率、故障原因、解决方案、使用寿命等维修记录；
g) 在关键领域或重要行业中电子信息产品在使用过程中采集、存储、管理和分析的涉及政府秘密、商业秘密和个人隐私的信息。包括地理地貌、气候环境、卫星轨道、军事部署等相关信息，企业、单位决定不宜公开的商业资料以及个人隐私包括个人身份信息、财产信息、健康信息等。

A.7.钢铁

主管部门：工业和信息化部。
重要数据包括但不限于：

A.7.1 钢铁产业的实力、潜力及竞争力信息

a) 重点区域或企业的生产安排、炼钢配比、规模、产量、生产设备与技术水平、采购计划、物流配送、能耗等信息；
b) 企业重点产品批量进入石油、化工等重点领域和新兴领域的信息；
c) 大型客户采购钢铁的品种、频次、吨数等信息。

A.7.2 国防军用和国民经济建设发展所需钢材、优特钢产业等实力信息

涉及冶金、能源、交通、建筑、桥梁、机械、电子等国民经济建设发展所需先进钢铁材料及其制品的信息。

A.7.3 国家产业发展及外部环境掌控、应对相关信息

a) 钢铁市场行情的预测和动态监测方面的信息；
b) 钢铁行业未公开的政策文件、布局安排、军民配置分配、统计数字等相关信息。

A.8. 有色金属

主管部门：工业和信息化部。

重要数据包括但不限于：

A.8.1 有色金属产业的实力、潜力及竞争力信息

a) 重点企业的生产安排、规模、产量、生产设备与技术水平、采购计划、物流配送、能耗、销售去向、贸易谈判等信息；
b) 大型客户采购有色金属的品种、频次、吨数等数据。

A.8.2 国防军工和国民经济建设发展所需有色金属信息

有色金属产品的名称、科研、勘察开采计划，生产能力、工艺技术路线，全部技术资料，企业名称、产地、产量、产能、储备、消费去向等信息及统计信息。

A.8.3 国家有色金属产业发展及外部环境掌控、应对信息

有色金属市场行情的预测和动态监测方面的信息。

A.9. 装备制造

主管部门：工业和信息化部。

重要数据包括但不限于：

A.9.1 投资信息

生产安全保障类装备和高技术关键装备，如军事、航空航天装备等的投资信息；

A.9.2 重要装备出厂后工程活动信息

国民经济、国防施工等重要领域装备长时间或大范围生产活动相关信息。

A.10. 化学工业

主管部门：工业和信息化部。

重要数据包括但不限于：

a) 国家主要化工产品生产能力、储备情况等统计信息，重大化工进出口项目相关信息；
b) 重要地区化工经济项目协议、项目、计划以及军用化学品出口相关信息等；
c) 剧毒化学品、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；
d) 生产、储存危险化学品的单位，其作业场所设置通信、报警装置、警卫保护措施等相关信息；
e) 机构出具的对化工企业的安全生产条件进行评价的报告；
f) 新建、改建、扩建生产、储存危险化学品的建设项目，及新建、改建、扩建储存、装卸危险化学品的港口建设项目信息；
g) 化工厂房平面图、化学品存储库房分布、库场面积、容量、年度用量、来源等资料；
h) 企业生产、储存的剧毒化学品、易致爆危险化学品的数量、流向等相关信息。

A.11. 国防军工

主管部门：国防科工局。

其重要数据包括但不限于：

a) 采购元器件、软件、型号材料、工控设备测试仪器的名称、数量、来源、途径、代理商等信息；
b) 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。

A.12. 其它工业

主管部门：工业和信息化部。

重要数据包括但不限于：

a) 战争及临时宣布的紧急备战时期，全国及各大地区军用产品的运输、储备计划和执行情况；
b) 处于世界先进水平，且对国民经济具有重要影响的工业研究开发项目、计划；
c) 具有国际水平和重大经济效益的科研成果中的核心部分；
d) 全国输油、输气管线及战备油库的坐标；
e) 全国石油库存的分布、统计数字及有关资料；
f) 涉及国防军工生产的发供用电规划、计划和统计资料；
g) 工业科技发展重点任务中与安全相关的关键科技内容。

A.13. 地理信息

主管部门：国土资源部（国家测绘地理信息局、国家海洋局）。

重要数据包括但不限于：

A.13.1 重要目标地理信息

a) 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；
b) 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；
c) 分辨率和位置精度优于遥感影像公开使用要求的影像；
d) 大于1:5万（含）比例尺海图及其数字化成果；
e) 大于1:5万（含）比例尺地形图及其数字化成果；
f) 未经审核发布的重要地理信息，包括国界、国家海岸线长度；领土、领海、毗连区、专属经济区面积；国家海岸滩涂面积、岛礁数量和面积；国家版图的重要特征点，地势、地貌分区位置；国务院测绘地理信息行政主管部门商国务院其他军地有关部门确定的其他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；
g) 地理信息分析数据，包括能源、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。

A.13.2 标识有下列内容的（对社会公众开放的除外）地理信息

a) 专用铁路及站内火车线路、铁路编组站，专用公路；
b) 未经国家有关部门批准公开发布的与地理相关的重大经济建设信息等；
c) 未公开的机场（含民用、军民合用机场）和机关、单位的信息；
d) 国家法律法规、部门规章禁止公开的其他内容。

A.13.3 标识有下列目标具体形状及属性的（用于公共服务的设施可以标注名称）地理信息

a) 大型水利设施、电力设施、通信设施、石油和燃气设施、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；
b) 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；
c) 公开机场的内部结构及运输能力属性；
d) 渡口的内部结构及属性；
e) 国家法律法规、部门规章禁止公开的其他内容相关形状和属性。

A.13.4 标识有下列内容属性的地理信息

a) 高压电线、通信线、管道的属性；
b) 国家法律法规、部门规章禁止公开的其他内容相关属性；
c) 水库库容、输电线路电压等精确数据，桥梁、渡口、隧道的结构形式和河底性质，未经公开的港湾、港口、沿海潮浸地带的详细数据；
d) 重要桥梁的限高、限宽、净空、载重量和坡度属性，重要隧道的高度和宽度属性，公路的路面铺设材料属性；
e) 江河的通航能力、水深、流速、底质属性，水库的库容属性，拦水坝的构筑材料和高度属性，水源的性质属性，沼泽的水深和泥深属性。

A.13.5 特殊测绘信息

a) 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、海洋重力测量成果以及小于5’×5’分辨率的平均重力异常和似大地水准面成果等各类计算衍生产品；
b) 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；
c) 境内优于25米网络的数字高程模型、数字地表模型数据。

A.13.6 公开地图数据

按照2015年12月颁布的《地图管理条例》（国务院第664号令），互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并将互联网服务单位收集、使用、提供的用户位置相关信息存放在中华人民共和国境内。

A.13.7 北斗卫星导航信息

a) 北斗卫星导航系统的灾备和服务能力等数据；
b) 北斗卫星导航系统生成和服务的高精度位置数据；
c) 北斗卫星导航用户名录、属性、装备识别号（ID）及短信息服务内容等数据。

A.14. 民用核设施

民用核设施主管部门：国防科工局和能源局。
民用核设施安全监管部门：环境保护部（国家核安全局）。
重要数据包括但不限于：

A.14.1 民用核设施安全监管信息

a) 管理部门对于建造、装料、运行、退役等活动审批中涉及到的关键设计资料、运行参数等；
b) 未公布的全国辐射环境监测原始信息。

A.14.2 民用核设施运行信息

a) 核燃料生产、加工、贮存和后处理设施、放射性废物处理设施中涉及到的关键技术电子资料，如关键设备设计图纸、制造工艺等信息；
b) 核动力厂（核电站、核热电厂、核供气供热厂等）的产能，核燃料年度采购处置数量及处置信息，业务信息系统中重要业务统计信息，日常运维管理信息（如重大核电厂运行异常大事件、停堆换料或检修等）；
c) 其他反应堆（研究堆、实验堆、临界装置等）的使用信息、核燃料年度采购处置数量及处置信息，业务信息系统中重要业务数据统计信息，日常运维管理的信息（如停堆换料或检修等）；
d) 核燃料生产、加工、贮存和后处理设施的年度处理能力、年度处理记录、原料采购、产品销售等相关统计信息、业务系统中的业务信息；
e) 放射性废物处理和处置设施的年度处理能力、年度处理记录、原料采购、产品销售等相关统计信息，业务系统中的业务信息；
f) 核动力厂、反应堆、核燃料加工处理等机构为满足监管要求建立的通信网络相关信息，以及上报的停堆换料或检修等信息；
g) 对核设施工况参数进行监控而使用的核设施数据采集系统形成的信息。

A.14.3 核设施产业发展信息

a) 我国核原料矿产分布、储量等信息；
b) 国家发展规划中关于民用核设施的发展规划信息；
c) 民用核设施科研中的试验或测试数据。

注：依据我国有关法律法规以及参加的国际公约，以上信息中已公开的除外。

A.15. 交通运输

主管部门：国家交通战备办公室、交通运输部、国家铁路局、中国铁路总公司。
重要数据包括但不限于：

A.15.1 含有下列内容，或通过汇聚分析能印证、推论出下列信息的数据

交通运输相关的信息通信系统部署信息、无线电频谱（有公开标准、依照国家公约、国内法律法规规定的除外）。

A.15.2 以下各个具体领域的属性数据单点可被测定或公开，但集中批量的数据泄露可能会危害国家安全、军事行动或反恐安全

a) 关键铁路线路图、车站布局、轨道分布、仓储数据等资料；
b) 涉外交通运输工程施工建设过程中的地理、水文、技术资料、统一口径等数据。

A.16. 邮政快递

主管部门：邮政局。
重要数据包括但不限于：
a) 与客户签署保密协议或协议中保密条款约定的不能共享使用的信息；
b) 邮政服务过程中的名址、联系电话、数量金额等信息；
c) 邮政企业、快递企业的运单数据，如收寄物品的名称、规格、数量、重量、收寄时间、寄件人和收件人名址、联系电话，以及寄递过程中的实时位置、位置轨迹、车辆、人员等信息；
d) 邮政企业、快递企业收集的上下游用户相关名址数据，涵盖企业、个人客户的客户名单、客户姓名或单位名称、网址或地址、联系电话等信息；
e) 收寄邮件、快件时登记的上下游用户实名身份证件信息；
f) 通过大数据分析得到涉及特定个体用户数据，如姓名、住址、身份证号、联系方式等；
g) 有助于黑客实施攻击邮政行业的数据，与基础设施、网络、系统等方面相关的材料，包括但不限于系统架构设计说明文档、基础设施的布局和建设文档、网络架构设计文档、IP地址分配文档、主要软硬件类型、维护人员信息、维护用户帐号和密码等。

A.17. 水利

主管部门：水利部。
重要数据包括但不限于：
a) 水情信息拍报电码；
b) 未经国际防汛抗旱总指挥部批准公布，可能造成重大灾情的水、旱情信息及预报成果；
c) 大型及防洪重点水库运行管理资料；
d) 大型水利水电、水利枢纽、跨流域调水等重要工程项目的规划、项目建议书、可行性研究、初步设计、施工、竣工验收报告、图纸等资料及系统水文分析成果；
e) 省、流域机构水利发展的中、长期计划；
f) 七大江河流域及重要地区水的中、长期供求计划；
g) 涉及对外技术合作和水利工程合作项目的未公开出版的科技成果、资料；
h) 反映大、中型水库移民生活困的资料及水库移民专项资金的年度计划；
i) 水文、水质年鉴、水情年报、水情资料汇编和水文公报（含水质通报、水资源公报等）；
j) 传输网络中的实时水文与工程运行信息；
k) 省际水事纠纷及水事违法案件、水土保持重要案件的正式资料；
l) 水利行政主管部门发布前的水利统计年鉴、资料汇编；
m) 全国江河湖泊水文观测数据，统计整编和分析的水文数据等。

A.18. 人口健康

主管部门：卫生计生委。
重要数据包括但不限于：
a) 在药品和避孕药具不良反应报告和监测过程中获取的个人隐私、患者和报告者信息；
b) 突发公共卫生事件与传染病疫情监测过程中获取的传染病病人及其家属、密切接触者的个人隐私和相关疾病、流行病学信息等；
c) 医疗机构和健康管理服务机构保管的个人电子病历、健康档案等各类诊疗、健康数据信息；
d) 人体器官移植医疗服务中人体器官捐献者、接受者和人体器官移植手术申请人的个人信息；
e) 人类辅助生殖技术服务中精子、卵子捐献者和使用者以及人类辅助生殖技术服务申请人的个人信息；
f) 计划生育服务过程中涉及的个人隐私；
g) 个人和家族的遗传信息；

h) 生命登记信息。

A.19. 金融

主管部门：人民银行。

重要数据包括但不限于：

A.19.1 金融机构安全信息

a) 新产品研发方案以及研发过程中产生的相关记录和数据；
b) 技术方案、电路设计、计算机软件、源代码和目标码、数据库、研究开发记录、技术报告、检测报告、实验数据、实验结果、图纸等技术文档；
c) 产品销售信息、市场调研信息、市场营销计划、财务资料、业务分析研究成果等经营资料；
d) 客户名单、客户身份资料、客户交易记录等客户资料；
e) 内部安全保卫制度、操作细节、银行业务使用的密押、编制方案及专用暗记、代号、指令密码；
f) 其他一经泄露会对各金融机构安全和利益造成损害的信息。

A.19.2 自然人、法人和其他组织金融信息

a) 个人财产信息。包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等；
b) 账户信息。包括银行结算账户和支付账户的信息。主要要素为：账号名称、账号、账户类型、账户开立时间、开户机构、绑定账户信息、账户验证信息（含客户身份外部渠道验证信息）、账户映射的敏感介质信息（如银行卡有效期、验证码、磁道信息等）、账户余额、账户交易情况等；
c) 个人信用信息。包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息；
d) 自然人、法人和其他组织金融交易信息。包括银行业金融机构、证券业金融机构、保险业金融机构、交易及结算类金融机构、非银行支付机构等各类金融机构办理业务时获取的自然人、法人和其他组织交易信息；
e) 身份信息。包括个人身份信息和单位身份信息。其中个人身份信息包括个人姓名、性别、国籍、民族、身份证种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等。单位身份信息包括单位名称、统一社会信用代码、类型、法定代表人（负责人）姓名及身份证件号码、经营场所、联系方式等；
f) 衍生信息。包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息；
g) 在与自然人、法人和其他组织建立业务关系过程中获取、保存的其他自然人、法人和组织信息。

A.19.3 中央银行、金融监管部门、外汇管理部门工作中产生的不涉及国家秘密的工作秘密。

A.20. 征信

主管部门：人民银行。

重要数据包括以下内容：

a) 法院生效判决、裁定、调解和执行信息；
b) 欠缴税收信息；
c) 欠缴劳动及社会保障保险信息；
d) 行政事业性收费、政府性基金欠费信息；
e) 公共事业欠费信息；
f) 信用卡还款情况、贷款偿还情况；
g) 企业和个人与金融机构以外的市场主体发生融资授信关系产生的信息，包括商业信用信息、民间借贷信息和水电费欠费信息等。

A.21. 食品药品

监管部门：食品药品监管总局。

重要数据包括但不限于：

a) 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，例如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；
b) 第二类、第三类医疗器械临床试验数据/报告；
c) 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；
d) 食品药品安全重大（紧急）信息。包括事件发生时间、地点、当前状况、危害程度、先期处置、发展趋势、事件进展、后续应对措施、调查详情、原因分析；
e) 大宗粮食加工品（含大米、小麦粉等）抽检监测信息。

A.22. 统计

主管部门：统计局。
重要数据包括但不限于：

A.22.1 人口

a) 人口普查的资料（包括姓名、性别、年龄、民族、户口登记状况、受教育程度、行业、迁移流动、社会保障、婚姻、生育、死亡、住房情况等）；
b) 人口普查中获得的能够识别或者推断单个普查对象身份的资料。

A.22.2 经济

a) 全国国内生产总值（GDP）初步核算数；
b) 全国规模以上工业总产值及增加值、主要财务指标；
c) 全国单位国内生产总值（GDP）能耗及其降低率；
d) 各省、自治区、直辖市单位地区生产总值能耗及其降低率、固定资产投资额、社会消费品零售总额等；
e) 各省、自治区、直辖市粮食、棉花总产量；
f) 全国粮食、棉花总产量；
g) 各省、自治区、直辖市工业生产者出厂价格指数及主要分类指数、购进价格指数及主要分类指数；
h) 全国工业生产者出厂价格指数及主要分类指数、购进价格指数及主要分类指数；
i) 全国及各省、自治区、直辖市主要工业产品产量；
j) 全国及各省、自治区、直辖市房地产开发投资额、销售额、销售面积、建筑业总产值、增加值；
k) 全国及各省、自治区、直辖市农林牧渔业总产值、农业生产资料价格指数、商品零售价格指数、固定资产投资价格指数及主要分类指数；
l) 全国及各省、自治区、直辖市煤炭等能源消费总量及其增长率；
m) 全国及各省、自治区、直辖市农村居民人均现金收入、人均纯收入、人均可支配收入、人均生活消费支出等；
n) 全国及各省、自治区、直辖市城镇居民人均可支配收入、人均消费支出；
o) 全国及各省、自治区、直辖市居民人均可支配收入、人均消费支出；
p) 其它与国家安全和经济利益密切相关的重要统计数据及统计分析材料；
q) 其它与全国或较大区域（一省或数省）社会秩序和经济秩序密切相关的重要统计数据及统计分析材料。

A.23. 气象

主管部门：气象局。
重要数据包括但不限于：
a) 我国气象卫星原始资料；
b) 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的观测气象数据；
c) 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；
d) 为高科技或者特殊科学试验研究获得的空间大气监测数据；
e) 为国家或者军事部门保密任务专门统计整编和分析的重要气象数据；

f） 通过非国际交换途径获得的各种国外气象数据；
g） 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、天气雷达、气象卫星数据及相应元数据，我国未公布的数值预报产品；
h） 专项、专业气象数据，包括海洋气象、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。

A.24. 环境保护

主管部门：环境保护部。
重要数据包括但不限于：
a） 未公布的长时间系列各行业（领域）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；
b） 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；
c） 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；
d） 未公布的全国土壤污染监测或调查数据。

A.25. 广播电视

主管部门：国家新闻出版广电总局。
重要数据包括但不限于：
a） 广播电视安全播出运维、应急保障、调度指挥等信息材料；
b） 广播电视监测监管系统产生的相关数据；
c） 广播电视台产生业务相关系统网络拓扑、安全运维类信息以及不宜公开的报道方案、媒体资源类文件等信息资料；
d） 广播电视无线和卫星传输覆盖网系统配置、播出参数及台站位置信息等重要数据；
e） 全国直播卫星用户信息。

A.26. 海洋环境

主管部门：国家海洋局。
重要数据包括但不限于：
a） 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；
b） 领海内的温盐、水声、底质、潮汐、海流实测数据和相关成果；
c） 未公布的海洋生态环境监测数据。

A.27. 电子商务

主管部门：商务部。
重要数据包括但不限于：
a） 个人在电子商务平台的注册信息，包括姓名、性别、年龄、住址、婚姻、学历、职业、收入、账户、联系方式等；
b） 企业在电子商务平台的注册信息，包括企业名称、住址、证照编号、经营范围、账户、联系方式等；
c） 电子商务交易记录以及相关的个人消费习惯及偏好和企业经营数据等；
d） 电子商务交易记录以及相关的个人消费习惯及偏好和企业经营数据等；
e） 电子商务交易各方的信用记录和信用评价信息；
f） 电子商务平台企业的经营数据；
g） 电子商务相关服务信息，包括支付和融资信息、物流信息等；
h） 对上述数据进行加工形成的涉及国计民生的全国或区域经济运行、行业发展情况的统计分析报告等。

A.28. 其它

重要数据涉及范围众多，本指南仅列出部分行业（领域）重要数据部分范围或内容，其它重要数据可依据下列规则判断、识别：

a) 企事业单位掌握的能够反映国家某行业（领域）整体情况的数据，且该行业（领域）与国家安全、社会公共利益密切相关；
b) 反映能够导致某行业（领域）发生系统性风险的企事业单位总体运行状况的数据，以及一旦完整性、保密性、可用性遭破坏即能显著影响这些单位稳定运行的各种数据；
c) 反映不可更改或长时间保持稳定的自然、经济、社会特征的数据，如地理位置、地貌特征、矿区位置、民族基因特性等；
d) 在各类数据集合并过程中能起到识别、关联、连接作用的数据，如地理位置、身份证号、手机号、法人代码；
e) 各行业主管部门在重大规划、计划、决策中所依赖或从本行业（领域）的企事业单位调取的部分数据；
f) 行政机关、执法机关在履职、执法过程中收集、产生的可能影响国家安全、社会公共利益或存在大量个人隐私的信息；
g) 单条或少量信息不会影响国家安全或社会公共利益，但覆盖较大范围或较长时间，一旦出境会带来危害或影响的某些信息集合；
h) 单条或少量信息不会影响国家安全或社会公共利益，但涉及某些重要区域或时期，一旦出境会带来危害或影响的某些信息集合；
i) 关键信息基础设施的系统设计、安全防护计划和策略方案，及其单元或设备选型、配置、软件等属性信息和脆弱性信息等；以及包括密码技术在内的其它与国家安全相关的单元、装置、设备、系统或计划、设计能力和缺陷信息；
j) 与意识形态、舆情等有关的文化安全相关信息；

行业（领域）主管部门可根据行业（领域）发展、评估实践，判断是否存在其它重要数据并及时更新指南。

附 录 B
（规范性目录）
个人信息和重要数据出境安全风险评估方法

B.1 评估个人信息出境对个人权益产生的影响等级

B.1.1 个人信息类型和敏感程度

个人信息因其敏感程度、出境后的处理目的等不同，对个人权益可能造成的影响有所不同，出境后的个人敏感信息如出现泄露、毁损、篡改或滥用等情形时，对个人合法权益造成的影响通常高于非敏感类个人信息。

B.1.2 个人信息数量

个人信息数量越大，或涉及特定群体的个人信息数量越多，当安全事件发生时，对个人权益造成的影响会随之增加，甚至影响国家安全和社会公共利益。

B.1.3 个人信息范围

个人信息范围超出与出境目的相关联的最小集时，将会对个人权益造成额外的影响。

B.1.4 个人信息技术处理情况

网络运营者可在满足业务需求的前提下，对拟出境的个人信息采取去标识化等脱敏技术处理措施，且应对去标识化后个人信息能否再次识别出个人信息主体进行验证，确保达到合理程度的不可逆，经技术处理后的个人信息能有效降低数据出境安全风险。

B.1.5 个人权益影响等级判定

评估个人权益受影响等级时，首先，需要对其关键要素个人信息敏感程度进行分析，初步判定影响等级；其次，根据个人信息数量、个人信息范围、技术处理情况、数据频率和其他数据特征等要素对影响等级进行进一步修正，使其更加准确。

为了方便分析和计算，个人权益受影响等级的判定可采用半定量方式，其中判定方法参考下表：

表 B.1 个人权益受影响等级判定表

关键要素	影响等级	修正要素		
敏感程度		数量	范围	技术处理情况
个人敏感信息为主	3	一年内涉及出境的个人信息大于 50 万人，影响等级可增加 1。	如果出境个人信息超出满足出境目的最小元素集，则影响等级可增加 1。	使用技术措施对涉及出境的个人信息进行去标识化处理，能有效防止识别出个人的，影响等级可减去 1。
包含少量个人敏感信息	2			
仅为个人信息，且不包含个人敏感信息	1			

B.2 评估重要数据出境对国家安全、社会公共利益产生的影响等级

B.2.1 重要数据类型

重要数据出境后如出现泄露、毁损、篡改或滥用等情形，将损害国家安全和社会公共利益。

B.2.2 重要数据数量

重要数据其所蕴含的社会、经济价值，数量越大，发生泄漏、毁损、篡改或滥用时，对国家安全和社会公共利益危害程度越大。

B.2.3 重要数据范围

重要数据超出与出境目的相关联的最小集时，将会对国家安全和社会公共利益造成额外的影响。

B.2.4 重要数据技术处理情况

重要数据在出境前，网络运营者应对其采取脱敏等技术处理措施，并对脱敏处理的效果进行验证，保证达到了合理程度的不可逆效果。脱敏后的重要数据能适度降低出境带来的安全风险。

B.2.5 国家安全和社会公共利益受影响等级判定

评估国家安全和社会公共利益受影响等级时，首先，需要明确关键要素重要数据内容，以及其影响等级；其次，根据重要数据数量、重要数据范围和技术处理等要素对影响等级进行进一步修正，使其更加准确。

为了方便分析和计算，国家安全和社会公共利益受影响等级的判定可采用半定量方式，其中判定方法参考下表：

表 B.2 国家安全和社会公共利益受影响等级判定表

关键要素	影响等级	修正要素		
重要数据类别		数量	范围	技术处理情况
识别出的重要数据	4	出境的重要数据多于1000GB，影响等级可增加 1。	如果出境重要数据超出满足出境目的的最小元素集，则影响等级可增加 1。	使用技术措施对重要数据进行脱敏处理，能达到合理程度的不可逆，影响等级可减去 1。

B.3 评估安全事件的可能性等级

B.3.1 评估发送方的安全保障能力等级

根据数据发送方对技术保障要求和管理保障要求的实施情况，将保障能力等级划分为高、中、低三个等级。

表B.3 发送方安全保障能力赋值

类别	保障能力等级	具体描述
技术保障能力	高	发送方采用了数据传输保护、边界防护等总体安全防护技术手段，并建立数据出境日志留存机制，能够有效保护数据安全，如果被威胁利用，造成的损害可以忽略。
	中	发送方采用的数据传输保护、边界防护等技术手段存在可被利用的低等级缺陷，或日志留存机制不够完善，如果被威胁利用，将造成一般损害。
	低	发送方采用的数据传输保护、边界防护等技术手段存在较高等级缺陷，或未建立日志留存机制，无法有效保护数据安全，如果被威胁利用，将造成完全损害。
管理保障能力	高	发送方具备完备的管理制度、应急机制、审计机制、投诉与处置策略、安全事件上报机制等管理机制，能够有效保护数据安全，如果被威胁利用，造成的损害可以忽略。
	中	发送方具备基本的管理制度、应急机制、审计机制等管理机制，管理方式有待提升，如果被威胁利用，将造成一般损害。
	低	发送方不具备有效的管理制度、应急机制、审计机制等管理机制，管理手段缺失严重，数据泄露可能性极大，如果被威胁利用，将造成完全损害。

B.3.2 评估接收方的安全保障能力等级

根据数据接收方对技术保障要求和管理保障要求的实施情况，将保障能力等级划分为高、中、低三个等级。

表 B.4 接收方安全保障能力赋值

类别	保障能力等级	具体描述
技术保障能力	高	数据接收方具备较先进的安全技术能力，同时接收数据的信息系统符合所在国家或区域的安全等级防护要求，且具备支持数据安全保障的自动化工具，能够有效保护数据安全，如果被威胁利用，造成的损害可以忽略。
	中	数据接收方具备一定的安全技术能力，接收数据的信息系统基本符合所在国家或区域的安全等级防护要求，数据安全保护自动化能力存在欠缺，如果被威胁利用，将造成一般损害。
	低	数据接收方安全技术能力较弱，接收数据的信息系统未达到所在国家或区域的安全防护要求，完全不具备支持数据安全保障的自动化工具，无法有效保护数据安全，如果被威胁利用，将造成完全损害。
管理保障能力	高	数据接收方的组织建设健全、制度流程完备、人员能力良好，如果被威胁利用，造成的损害可以忽略。
	中	数据接收方的组织建设基本健全、制度流程较规范、人员能力一般，如果被威胁利用，将造成一般损害。
	低	数据接收方的组织建设不健全、制度流程缺失、人员能力较差，如果被威胁利用，将造成完全损害。
主体审查	高	数据接收方企业资质完备齐全，背景关系清晰，经营范围与接收数据的类型和内容完全一致，且无违法记录。
	中	数据接收方企业资质相对齐全，背景关系相对清晰，经营范围与接收数据的类型和内容基本一致，且无重大违法记录。
	低	数据接收方缺乏合法企业资质，经营范围与接收数据的类型和内容存在较大差异，或存在重大违法记录。

B.3.3 评估接收方所在国家或区域的政治法律环境

B.3.3.1 评估个人信息接收方所在国政治法律环境

个人信息接收方所在国政治法律环境评估是指对该国家或地区现行的个人信息保护法律、法规、标准情况，该国家或地区加入的区域或全球性的个人信息保护方面的机制以及所做出的具有约束力的承诺，该国家或地区落实个人信息保护的机制进行评估，依据各方面水平的高低，将保障能力等级划分为高、中、低三个等级。

表 B.5 个人信息接收方所在国家/地区政治法律环境赋值

类别	保障能力等级	具体描述
数据接收方所在国家/地区的政治法律环境	高	个人信息保护方面的法律法规标准较为成熟且已形成体系化，保障了个人在个人信息方面的各项权利，同时具备完备、有效、多层次的救济渠道。
	中	个人信息保护方面的法律法规标准基本齐备，保障了个人在个人信息方面的部分权利，具备相应的行政、司法救济渠道。
	低	个人信息保护方面的法律法规标准欠缺或不完备，个人仅能通过司法救济渠道维护权利。

B.3.3.2 评估重要数据接收方所在国政治法律环境

重要数据接收方所在国政治法律环境评估是指对评估重要数据接收方所在国家或地区的数据安全方面现行的法律法规和标准情况，该国家或地区落实数据安全的机制、该国家或地区政府在执法、国防、国家安全等部门调取数据的法律权力，该国家或地区与其他国家或地区之间有关数据流通、共享等方面的双边或多边协定进行评估。依据各方面水平的高低，将保障能力等级划分为高、中、低三个等级。

表 B.6 重要数据接收方所在国家/地区政治法律环境赋值

类别	保障能力等级	具体描述
数据接收方所在国家/地区的政治法律环境	高	网络安全或数据安全方面的法律法规标准完备，主管或监管部门具备较强的监督和执法能力，数据安全事件发生后具备多层次、多方面的有效追责和监督机制。政府调取数据的权力受法律的严格约束，且做到了公开透明，过往不存在相关的负面报道。
	中	网络安全或数据安全方面的法律法规标准基本完备，主管或监管框架初步成型，对数据安全事件主要依靠行政监督，政府调取数据需要遵循一定的程序，过往有少量的负面报道。
	低	网络安全或数据安全方面的法律法规标准欠缺或不完备，主管或监管部门不清晰或缺乏相应能力，缺乏在数据安全事件发生后有效追责的机制，政府调取数据的权力基本不受约束。

B.3.4 安全事件可能性等级判定

安全事件的可能性与发送方安全保障能力、接收方安全保障能力以及接收方所在国家或地区的法律环境有关，根据上述要素的分析与赋值，为了方便分析和计算，安全事件的可能性等级判定方法参考下表：

表 B.7 安全事件可能性等级判定表

可能性等级	判定条件
3	发送方技术保障能力、管理保障能力、接收方主体审查、技术保障能力、管理保障能力、政治法律环境任何一项赋值为“低”的。
2	发送方技术保障能力、管理保障能力、接收方主体审查、技术保障能力、管理保障能力、政治法律环境赋值有“中”和“高”的。
1	发送方技术保障能力、管理保障能力、接收方主体审查、技术保障能力、管理保障能力、政治法律环境所有项赋值均为“高”的。

B.4 安全风险综合评估

安全风险综合评估是根据国家安全、社会公共利益和个人权益受影响程度以及安全事件可能性两方面进行综合评价，分析数据出境活动整体的安全风险级别，安全风险级别划分为极高、高、中、低四个等级，对风险级别的判定可参考下表。

表 B.8 安全风险级别判定参考表

	安全事件可能性等级		
影响程度等级	1	2	3
≥5	高	极高	极高
4	中	高	高
3	低	中	高
2	低	中	中
1	低	低	中

参考文献

[1] ISO/IEC 27000-2013 信息安全管理体系 概述和术语
[2] ISO/IEC 27001-2013 信息安全管理体系 要求
[3] ISO/IEC 27002-2013 信息安全管理实用规则
[4] ISO/IEC 27003-2013 信息安全管理体系实施指南
[5] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
[6] GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求
[7] NIST Special Publication 800-53 联邦信息系统和组织的安全和隐私控制