

T/CIIA

中国信息协会团体标准

T/CIIA XXXX—XXXX

空间环境科学数据安全分级指南

Guidelines for space environment scientific data security classification

征求意见稿

（本草案完成时间：）

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。



版权所有归属于该标准的发布机构，除非有其他规定，否则未经许可，此发行物及其章节不得以其他形式或任何手段进行复制、再版或使用，包括电子版，影印件，或发布在互联网及内部网络等。使用许可可于发布机构获取。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

中国信息协会 发布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 安全分级原则 2

5 安全分级框架 2

6 安全分级流程与方法 3

7 安全级别变更 5

参考文献 6

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国信息协会提出并归口。

本文件起草单位：

本文件主要起草人：

CIIA

空间环境科学数据安全分级指南

1 范围

本文件提供了空间环境科学数据安全分级原则，给出了空间环境科学数据安全分级框架、流程与方法的建议。

本文件适用于科学数据管理机构、科研机构、行业机构及企业等法人单位对空间环境科学数据的分级管理和保护。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

空间环境 space environment

地表以上几十公里直至太阳表面之间的环境。

注：通常所说的空间环境指日地空间环境。

[来源：GB/T 30114.2-2014，7.1，有修改]

3.2

科学数据 scientific data

在自然科学、工程技术科学等领域，通过基础研究、应用研究、试验开发等产生的数据，以及通过观测监测、考察调查、检验检测等方式取得并用于科学研究活动的原始数据及其衍生数据。

[来源：科学数据管理办法第一章 第二条]

3.3

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

[来源：中华人民共和国数据安全法 第一章 第三条]

3.4

安全分级 security classification

根据数据安全遭到破坏对象产生的负面影响程度，将空间环境科学数据安全级别从高到低划分为不同等级的过程。

3.5

科学数据管理责任主体 responsible body of scientific data management

有关科研院所、高等院校和企业等法人单位。

[来源：科学数据管理办法 第二章 第九条，有修改]

3.6

保密性 confidentiality

信息对未授权的个人、实体或过长不可用或不泄露的性质。

[来源：GB/T 25069-2022，3.41]

3.7

可用性 availability

可由经授权实体按需访问和使用的性质。

[来源：GB/T 25069-2022，3.345]

3.8

完整性 integrity

没有遭受以未经授权方式所作的更改或破坏的特性。

[来源：GB/T 25069-2022，3.574，有修改]

3.9

真实性 authenticity

一个实体是其所声称的实体的性质。

[来源：GB/T 25069-2022，3.769]

4 安全分级原则

空间环境科学数据安全分级宜遵循以下原则。

- a) 合法合规性原则
满足国家法律法规及科学数据管理责任主体的有关规定。
- b) 可执行性原则
建议科学合理设置空间环境科学数据安全分级方法，且具有可操作性。
- c) 时效性原则
因科学数据生命周期不同阶段的价值、影响及保护要求不同，因此其安全分级宜具有一定的有效期限，建议按照级别变更策略对数据级别进行及时调整。
- d) 自主性原则
根据空间环境科学数据自身数据管理需要（如国家发展战略需要、学科前沿技术研究、科学数据管理业务需要、国防安全管理风险接受程度等），基于本文件的相关规定自主确定数据安全级别。
- e) 差异性原则
宜根据空间环境科学数据对象类别（如地磁数据、电离层数据、大气层数据）及敏感程度等差异，划分不同的数据安全层级，并赋予不同的安全等级。
- f) 客观性原则
宜通过数据特征属性（如数据精度、数据规模、数据内容涵盖的特定对象等）的测度，确定空间环境科学数据的相应等级，并且空间环境科学数据的定级是可复核和检查的。

5 安全分级框架

5.1 安全分级范围

科学数据中心、政府管理部门、行业、科研机构及企业所管理、所有和使用的空间环境科学数据包括：基础研究、应用研究、试验开发等产生的数据，以及通过观测监测、考察调查、检验检测等方式取得并用于科学研究活动的原始数据及其衍生数据。

涉及国家秘密的科学数据不在本文件分级范围内。

5.2 安全分级要素

5.2.1 概述

空间环境科学数据安全分级要素包括：

- a) 影响对象；
- b) 影响程度。

5.2.2 影响对象

空间环境科学数据安全遭受破坏后受到影响的对象包括：

- a) 国家安全；
- b) 公众权益；

- c) 个人权益；
- d) 组织合法权益。

5.2.3 影响程度

空间环境科学数据安全遭到破坏所产生的负面影响，按其程度宜划分为以下四种：

- a) 严重损害；
- b) 一般损害；
- c) 轻微损害；
- d) 无损害。

5.3 安全级别划分

依据空间环境科学数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度等因素，空间环境科学数据安全级别可划分为五级，具体见表1。

表1 空间环境科学数据安全级别

安全级别	说明
5	数据安全遭到破坏后，对国家安全造成损害，或对公众权益造成严重损害，但不影响危害组织合法权益、个人权益
4	数据安全遭到破坏后，对公众权益造成一般损害，或对组织或个人权益造成严重损害，但不影响国家安全
3	数据安全遭到破坏后，对公众权益造成轻微损害，或对组织或个人权益造成一般损害，但不影响国家安全
2	数据安全遭到破坏后，对组织或个人权益造成轻微损害，但不影响国家安全和公众权益
1	数据安全遭到破坏后，可能对组织或个人权益不造成损害或仅造成微弱影响，但不影响国家安全和公众权益

5.4 安全分级要素与安全级别的关系

安全分级要素与安全级别的关系见表2。

表2 空间环境科学数据安全分级要素与安全级别关系

影响对象	影响程度			
	严重损害	一般损害	轻微损害	无损害
国家安全	5	5	5	1
公众权益	5	4	3	1
组织合法权益	4	3	2	1
个人权益	4	3	2	1

6 安全分级流程与方法

6.1 安全分级流程

空间环境科学数据安全分级流程宜符合图1。

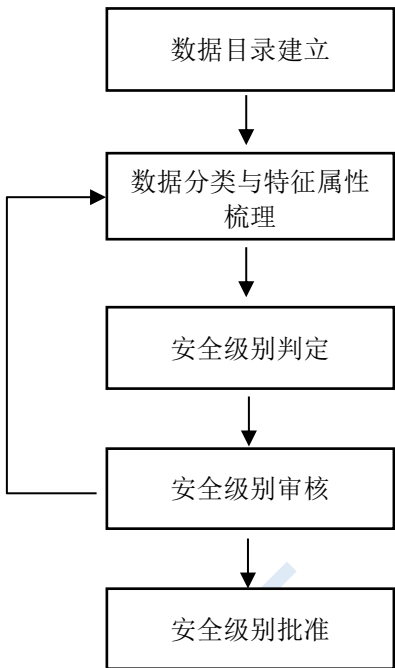


图1 空间环境科学数据安全分级流程

6.2 数据目录建立

对数据进行盘点与梳理，形成统一的数据目录。

6.3 数据对象分类与特征属性梳理

6.3.1 概述

对数据目录里的每一项数据产品或数据集进行分类，并依据数据类别梳理数据特征属性。

数据对象分类采用线分类法，大类按照观测区域划分。依据实际情况在大类框架下按观测要素/目标进一步划分中类。

6.3.2 数据对象分类

按观测区域可将空间环境科学数据对象划分为以下五类：

- a) 太阳-行星际；
- b) 磁层；
- c) 电离层；
- d) 大气层；
- e) 地表层。

6.3.3 数据特征属性

空间环境科学数据特征属性包括：

- a) 时空覆盖：包括地域覆盖、高度覆盖、时间覆盖等；
- b) 数据精度：包括时间分辨率、空间分辨率、数值分辨率等；
- c) 数据规模：包括数据体量、数据记录数等；
- d) 处理程度：包括原始数据、各级衍生数据等；
- e) 其他。

6.4 安全级别判定

6.4.1 概述

依据数据对象类别及特征属性的实际情况进行保密性、可用性、完整性和真实性评估，根据评估分析进行安全级别判定。

6.4.2 保密性评估

通过评价空间环境科学数据遭受未经授权的获取与使用后，对国家安全、公众权益、个人权益及组织合法权益所造成的影响进行数据保密性评估。

6.4.3 完整性评估

通过评价空间环境科学数据遭受未经授权的修改或损毁后，对国家安全、公众权益、个人权益及组织合法权益所造成的影响进行数据完整性评估。

6.4.4 可用性评估

通过评价空间环境科学数据及其经组合/融合后形成的各类数据出现访问或使用中断后，对国家安全、公众权益、个人权益及组织合法权益所造成的影响进行数据可用性评估。

6.4.5 真实性评估

通过评价空间环境科学数据遭受篡改、伪造和滥用后，对国家安全、公众权益、个人权益及组织合法权益所造成的影响进行数据真实性评估。

6.4.6 安全级别判定规则

安全级别判定宜考虑以下内容：

- a) 因不同数据在保密性、完整性、可用性、真实性方面有不同侧重，建议以所侧重的安全性评估结果作为主要的定级依据；
- b) 对于数据的保密性、完整性、可用性和真实性要求基本一致的，建议重点以保密性评估所确定的定级要素为主要定级依据。

6.5 安全级别审核

审核数据安全级别判定过程和结果，必要时重复6.3~6.4，直至安全级别划到与分级对象所在的科学数据管理责任主体的数据安全保护目标一致。

空间环境领域的核心数据和重要数据的识别及认定工作宜遵照国家及行业主管部门的有关规定。核心数据的安全级别不宜低于本文件规定的5级，重要数据的安全级别不宜低于本文件规定的4级。

6.6 安全级别批准

数据安全分级结果建议由科学数据管理责任主体的最高决策组织进行审议批准。

7 安全级别变更

安全级别变更建议由科学数据管理责任主体发起，并按数据安全分级流程实施。出现下列情形之一时，建议对数据安全级别进行变更。

- a) 数据内容发生变化，导致原有数据的安全级别不适用变化后的数据。
- b) 数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的数据安全级别不再适用。
- c) 因国家或主管部门要求，导致原定的数据安全级别不再适用。
- d) 因科学数据全生命周期流通过程中，经加工处理等导致数据内容发生变化，需要重新分级管理。
- e) 对于从多个数据源合并得到新的衍生数据，安全级别建议不低于原有最高级别。
- f) 需要对数据安全级别进行变更的其他情形。

参 考 文 献

- [1] GB/T 25069—2022 信息安全技术 术语
 - [2] GB/T 30114.2—2014 空间科学及其应用术语 第1部分：空间物理
 - [3] GB/T XXXX 科学数据安全分级分类指南
 - [4] 《中华人民共和国数据安全法》（中华人民共和国主席令第八十四号）
 - [5] 《科学数据管理办法》（国办发〔2018〕17号）
-

CONFIDENTIAL