ICS 07.040
CCS A 75

T B

团　　体　　标　　准

T/ CSGPC XXX—20XX

智能网联汽车时空数据 服务监管基本要求

Basic requirements for the supervision of spatio-temporal data services of intelligent connected vehicles

（征求意见稿）

（本稿完成时间：2023 年 12 月 1 日）

202x-xx-xx 发布　　202x-xx-xx 实施

中 国 测 绘 学 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。

本文件由中国测绘学会提出和归口。

本文件起草单位：

本文件主要起草人：

引　言

当前智能汽车新业态迅猛发展，为方便出行、减少污染、改善交通提供了有效的解决方案，其运行和服务高度依赖具有时间、空间或专题属性的时空数据，如智能汽车基础地图需要时空数据对地图进行更新；自动驾驶算法需要通过海量场景数据的训练进行更新迭代，不断优化；记忆泊车、寻车定位等地理信息位置服务需要车辆位置信息作为数据支撑。智能网联汽车时空数据是重要的战略性数据资源和新型生产要素，若不能规范使用，一旦泄露，将严重威胁我国地理信息安全。为规范智能网联汽车时空数据服务多场景应用，促进智能网联汽车时空数据有序使用，推动相关产业的健康有序发展，制定本文件。

智能网联汽车时空数据服务监管基本要求

1 范围

本标准规定了智能网联汽车时空数据服务提供者提供服务时的通用要求、服务要求和监管要求。

本标准适用于智能网联汽车时空数据服务提供者在多场景下提供的服务活动，也可供监管部门组织对智能网联汽车时空数据服务活动进行监督、管理和评估时参考。

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 20263 导航电子地图安全处理技术基本要求

GB/T 37092-2018 信息安全技术 密码模块安全要求

GB/T 37939-2019 信息安全技术 网络存储安全技术要求

GB/T 40861-2021 汽车信息安全 通用技术要求

GB/T 42517-2023 智能运输系统 智能驾驶电子道路图数据模型与表达

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能网联汽车时空数据 spatio-temporal data from ICV

智能网联汽车运行、服务和道路测试过程中产生的空间坐标、影像、点云及其属性信息等测绘地理信息数据。

3.2

智能网联汽车时空数据服务提供者 spatio-temporal data service provider

提供智能网联汽车时空数据服务的组织，通常包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

3.3

智能网联汽车时空数据服务场景 spatio-temporal data services scenario

对智能网联汽车时空数据服务提供者在提供智能网联汽车时空数据服务过程中的流程步骤、角色、交互过程等的描述，智能网联汽车时空数据服务场景通常包括导航电子地图制作、数据标注、算法研发、仿真测试和实车应用与测试等。

3.4

图商 map company

拥有导航电子地图制作测绘资质的企业。

4 通用要求

4.1 主体要求

时空数据服务提供者提供数据服务时,应依法取得相应测绘资质，或委托具有相应测绘资质的单位提供服务。

4.2 环境要求

4.2.1 时空数据的数据库服务器应设立在中华人民共和国境内。

4.2.2 提供时空数据服务的环境应符合《测绘资质管理办法》、《测绘资质分类分级标准》等有关法规标准要求。

4.3 人员要求

4.3.1 从事时空数据服务相关业务的人员应当拥有相关专业技能和知识，并签订保密责任书，接受保密教育并定期加强培训。

4.3.2 应建立健全时空数据安全保密制度，明确涉密人员管理，明确设置安全主管及安全管理的相关人员,并明确定义其职责范围。明确时空数据及其成果的使用审批流程和责任人，未经审计批准，任何人员不得将时空数据及其成果带离保密要害部位。

4.4 处理要求

4.4.1 提供时空数据服务时应符合测绘地理信息管理工作国家秘密范围、《导航电子地图安全处理技术基本要求》和《公开地图内容表示规范》等有关法规标准要求。

4.4.2 提供的时空数据涉及空间位置信息时,应采用经国家认定的空间位置保密技术处理。

4.4.3 应建立时空数据处理成果和资料档案管理制度，并向所在地监管部门报备。应对时空数据服务情况进行登记并长时间保存，实行可追溯管理。

4.4.4 向境外提供时空数据服务的，应履行数据出境安全评估和对外提供审批程序。

4.5 应急要求

4.5.1 制定时空数据服务安全事件应急预案，根据事件等级明确应急响应责任分工、工作流程和处置措施等。

4.5.2 制定时空数据服务安全事件应急演练计划，针对数据泄露、丢失、窃取、损坏、滥用、篡改、非法访问和违规传输等典型数据安全事件定期开展演练，形成演练总结报告。

4.5.3 发生时空数据服务安全事件后，按照应急预案及时开展应急处置，事件处置完成后，形成总结报告并及时上报。

4.5.4 涉及重要数据和核心数据的时空数据服务安全事件，及时上报，同时开展事态跟踪分析，并及时采取相关措施降低事件影响。

5 服务要求

5.1 导航电子地图场景

5.1.1 导航电子地图是指制作含有空间位置地理坐标，能够与空间定位系统结合，准确引导人或交通工具从出发地到达目的地的电子地图或数据集。

5.1.2 时空数据服务提供者提供时空数据用于导航电子地图制作的，应确保数据接收方具有导航电子地图制作资质或数据接收方出具委托相应资质单位开展导航电子地图制作的证明。

5.1.3 时空数据服务提供者利用持有的时空数据进行导航电子地图制作的，自身应具有导航电子地图制作资质或委托相应资质单位开展导航电子地图制作。

5.1.4 开展导航电子地图制作的单位应建立专门的导航电子地图数据处理物理环境，配置符合要求的安全保密专用产品，包括身份鉴别、访问控制、安全审计、保密技术防护（三合一）、漏洞扫描、计算机病毒查杀、边界安全防护和数据库安全等产品。存储介质应安排专人管理，建立台账。

5.1.5 应符合国标GB/T 42517-2023的要求。

5.2 数据标注场景

5.2.1 数据标注指使用几何标记和其他结构为数据生成时空描述使其比标签拥有更加丰富信息的过程。标签是向任何信息容器（如图像、视频或测试场景）添加简单和复杂语义标记的过程，是专业化的注释过程。

5.2.2 不应标注涉军单位和设施，宜将涉军涉敏单位统一归类处理。

5.2.3 应在可监控的环境下进行，通过部署安全网关、绑定标注账号、实时视频监控等技术或物理手段保障标注办公空间环境具备防下载、防拷贝、防拍照、防截图等安全能力，确保数据标注服务平台上的数据不会泄露。

5.3 算法研发场景

5.3.1 算法研发指通过研发先进的算法，实现车与人、车、路、云等智能信息的交换共享，具备复杂环境感知、智能决策、协同控制等功能，以实现安全、舒适、节能、高效行驶的新一代汽车研发过程。

5.3.2 不应开展可识别涉军单位和设施的算法研发，宜将涉军涉敏单位统一归类识别。

5.3.3 算法研发应在图商监管环境中进行，未脱敏时空数据不应离开图商监管环境。

5.4 仿真测试场景

5.4.1 仿真测试指使用计算机模型和虚拟环境来模拟和评估智能网联汽车系统的性能、安全性和可靠性的过程。

5.4.2 仿真测试可在图商提供的监管环境中进行，未脱敏时空数据不应离开图商监管环境。

5.5 实车应用与测试场景

5.5.1 指在实际道路环境中，对智能网联汽车进行的一系列应用与测试活动。

5.5.2 进行实车应用与测试时，应由图商负责智能网联汽车时空数据全生命周期安全。

5.5.3 应用与测试过程中产生的智能网联汽车时空数据的存储和传输应采用国家密码管理部门认定的密码技术进行加密。

6 监管要求

6.1 监管部门

各级自然资源部门为智能网联汽车时空数据服务的监管部门，负责具体的监管实施。

6.2 数据安全管理体系

6.2.1 时空数据服务提供者应建立时空数据安全管理体系。

6.2.2 时空数据安全管理体系中应涵盖必要流程，以确保充分考虑安全风险。

a) 应建立时空数据安全的内部管理流程，并向监管部门报备。
b) 应建立识别、评估、分类、处置时空数据安全风险及核实已识别风险是否得到适当处置的流程，并确保时空数据安全风险评估保持最新状态。
c) 应建立针对时空数据传输中窃听、攻击造成数据泄露的监测、响应及上报流程。
d) 时空数据安全管理制度、时空数据服务管理规范、时空数据安全监测制度、时空数据安全应急响应机制、时空数据安全事件管理规范等。

6.3 安全检查

6.3.1 被检查方应每半年向监管部门提交一次自查报告并随时准备接受监管部门的临时抽查，包括章节 6.2 的内容和必要的数据支持，监管部门组建具备高级专业资格的人员团队开展常规检查。

6.3.2 在发生安全威胁或者发生数据泄露事件后，被检查方应向监管部门报告事件情况，并配合监管部门进行调查及整改，监管部门组建具备数据安全事件处理经验的专业人员团队执行特殊检查。

6.4 应急处置

时空数据服务提供者在发送安全威胁或数据泄露事件后应向监管部门提交：安全威胁或数据泄露内容报告、事件原因分析报告、应急措施报告和数据安全整改措施报告等。

参考文献

[1] 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
[2] GB 20263-2006 导航电子地图安全处理技术基本要求
[3] GB/T 37092-2018 信息安全技术 密码模块安全要求
[4] GB/T 37939-2019 信息安全技术 网络存储安全技术要求
[5] GB/T 40861-2021 汽车信息安全 通用技术要求
[6] GB/T 42517.2-2023 智能运输系统 智能驾驶电子道路图数据模型与表达 第2部分：开放道路