《可信智能体空间建设指南
第1部分：总体架构与安全要求》
技术要求标准编制说明

可信智能体空间建设指南
技术要求标准起草组

1、标准范围。

本文件规定了可信智能体空间建设指南技术要求，包括四方面：一是可信智能体空间的总体架构，二是可信数据空间功能要求，三是可信数据空间安全性要求，四是可信数据空间业务流程及评估方法。

本标准适用于：

a）可信智能体空间服务提供方开展自评估与能力建设；

b）可信数据空间应用方或管理方对服务提供方的服务能力提出要求；

c）第三方机构对可信数据空间服务提供方进行能力评估与认证。

2、工作简况。

2025年7月，根据中国互联网协会团体标准管理规定，标准草案经审批予以立项。起草组由清雁科技（北京）有限公司、中国信通院、北京航空航天大学、山东省征信有限公司、中国交通信息科技集团有限公司、山东省港口集团有限公司、上海明品医学数据科技有限公司、河北清华发展研究院、中国民航科学技术研究院等家单位组成，召开 3 次技术讨论会、2 次公开征求意见会，形成本征求意见稿。

3、标准编制原则和确定标准主要内容的依据：

标准原则：本标准遵循“科学性、实用性、规范性”等原则，在确定标准主要内容和条款先进性的前提下，按照《标准化工作导则第1部分：标准化文件的结构和起草规则》（GB/T 1.1-2020）给出的规则进行编制，力求各项内容科学合理，符合政府大模型建设实际需求,并注重标准的可操作性。

标准内容：1.功能完备性，覆盖智能体注册、发现、调用、清算全生命周期。2.性能要求，并发 10 万智能体，端到端时延≤5 ms。3.安全性，落实等级保护、数据安全、个人信息保护、跨境合规、零信任架构全链条要求。4.服务能力，在可靠性、稳定性、可维护性、可扩展性、易用性五个方面提出可验证条款。5.兼容性，连接器 SDK 开源，兼容主流 OS、数据库、云平台。支持与现有云计算、大数据、区块链、TSN/DetNet 设备互联互通。6.可落地性，提供测试床、参考实现、评估工具，确保标准可验证、可复现、可推广。

4、主要试验（或验证）的分析、综述报告。

无。

5、标准在起草过程中遇到的问题及解决办法：重大分歧意见的处理经过和依据：有无重要技术问题需要说明。

本标准在起草过程中未遇到重大分歧意见，无重要技术说明。

6、与国外标准的关系：包括：采用国际标准和国外先进标准的程度，国外标准主要技术内容的差异（可引用标准前言的内容）：

无。

7、修订标准时，说明与标准前一版本的重大技术变化，并列出所涉及的新、旧版本的有关章条（可引用标准前言的内容）：废止/ 代替现行有关标准的建议：

不涉及。

8、说明标准与其他标准或文件的关系（可引用标准前言的内容），特别是与有关的现行法律、法规和强制性国家标准的关系：

《可信智能体空间建设指南》符合现行法律、法规要求。

9、标准作为强制性标准或推荐性标准的建议：

建议作为推荐性标准。

10、贯彻国家标准的要求和措施建议（包括组织措施、技术措施、过渡办法等内容）：标准发布后，对国内外业界可能产生的影响。

《可信智能体空间建设指南》的发布将规范智能体跨域协同与可信流通市场，显著提高智能体平台的技术水平、数据质量和算力调度效率，保障科研成果的准确性与可靠性，推动面向智能制造、智慧城市、车联网等场景的深入应用与创新。同时，该标准将贯通芯片、算力、网络、可信空间、密态计算等上下游环节，形成完整产业生态，带动链上企业协同发展。对国际业界而言，它集中展示了我国在智能体可信数据与确定性网络融合领域的技术规范与创新成果，为国际交流与合作提供了可复制的标准依据，显著提升我国在全球智能体可信协同领域的话语权和影响力，促进国际间技术与标准的深度对接。

11、标准是否涉及知识产权的情况说明；如标准中含有自主知识产权，说明产品研发程度、产业化基础及进程。

不涉及。

12、其他应予说明的事项。

无。