

团体标准《信息安全技术 大数据安全等级保护测评指引》

编制说明

一、工作简况

1.1 任务来源

根据中关村信息安全测评联盟2020年同意批准的《中关村信息安全测评联盟团体标准制修订立项申请书》，公安部信息安全等级保护评估中心负责标准制定项目《信息安全技术 大数据安全等级保护定级及测评工作指南》。

1.2 主要起草单位和工作组成员

公安部第三研究所（公安部信息安全等级保护评估中心）主要负责起草，深圳市网安计算机安全检测技术有限公司、浙江东安检测技术有限公司、山东建筑大学、深圳市信息安全管理中心、中国软件评测中心、山东新潮信息技术有限公司、贵州省信息与计算科学重点实验室、国家信息技术安全研究中心等单位共同参与了该标准的起草工作。

1.3 确定编制内容

标准编制组以网络安全测评工作实践为基础，以 T/ISEAA 002-2021《信息安全技术 大数据安全等级保护基本要求》、GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》为主要参考依据，规定了网络安全等级保护第二级到第四级大数据等级保护对象的安全测评方法和要求，完成《信息安全技术 大数据安全等级保护定级及测评工作指南》标准的编制工作。包括：

（1）依据 T/ISEAA 002-2021《信息安全技术 大数据安全等级保护基本要求》条款，给出各要求项的单项测评实施方法；

（2）明确大数据系统的等级保护对象存在形态；

（3）针对大数据系统这类特殊的测评对象，给出测评中需要特殊关注和注意的测评实施要点，包括系统调研、测评对象确定、测评指标确定、测评实施关注点等。

1.4 主要工作过程

1.4.1 草案

2021年9月至2021年10月，标准编制组人员首先对所参阅的文献、标准等资料进行查阅和理解，编写标准编制提纲，并在对提纲进行修改完善的基础上，开始具体的编制工作。

2021年11月至2022年1月，标准编制组按照计划调研了国际和国内大数据安全保护及安全测评情况，分析并总结了大数据安全保护的安全关注点和要素，可能面临的重大风险，安全保护工作要求等；同时标准编制组调研了与该标准相关的其他国家标准和行业标准，完成了《大数据安全等级保护定级及测评工作指南编制研究报告》。

2022年2月至2022年7月标准编制组在前述工作成果《信息安全技术 大数据安全等级保护定级及测评工作指南编制研究报告》的基础上，以编制组人员收集的资料为基础，在不断的讨论和研究中，完善内容，形成了本标准草案前四章以及第三级安全测评要求的内容，并召开工作组研讨会，针对已有内容进行研讨，并在内部统一意见建议将标准名称改为《网络安全等级保护大数据测评指南》。

2022年8月至2022年12月，标准编制组进一步修改完善标准已有内容，并在第三级安全测评要求基础上完成了第二级以及第四级安全测评要求，形成了《网络安全等级保护大数据测评指南》标准草案。

2023年1月至2023年3月，标准编制组在编制组涉及单位内部征求标准草案意见，并根据意见修改完善，形成了新一版《网络安全等级保护大数据测评指南》标准草案。

二、标准编制原则和确定主要内容的论据及解决的主要问题

标准编制的基本原则是配合《中华人民共和国网络安全法》（以下简称“网络安全法”）的实施，进一步推进网络安全等级保护工作的开展，进一步适应信息技术的发展。基于上述原则并依据T/ISEAA 002-2021《信息安全技术 大数据安全等级保护基本要求》，针对大数据系统提出安全测评扩展要求。

1. 标准编制原则和目的

《信息安全等级保护管理办法》（公通字[2007]43号）明确指出信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，而且等级测评的技术测评报告是其检查内容之一。这就要求等级测评过程规范、测评结论准确、公正及可重现。

《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）（简称《基本要求》）和《信息安全技术 网络安全等级保护测评要求》（GB/T28448-2019）（简称《测评要求》）等标准对近几年来全国网络安全等级保护工作的推动起到了重要的作用。

伴随着IT技术的发展，大数据技术应用越来越广泛，《测评要求》针对大数据类等级保护对象的测评内容尚不全面，因此需要通过吸取国际、国内先进的大数据安全测评经验和相关内容，结合我国大数据技术应用特点、网络安全领域的保护及测评现状，为大数据等级保护对象落实法律法规要求的网络安全等级保护测评工作提供方法和技术支撑，制定出具有指导意义的安全标准文档，为规范大数据安全测评工作提供依据。同时，本项目的研究将进一步推动我国对大数据安全保护相关理论的研究，促进我国大数据保护工作的开展，对促进大数据安全测试评估的技术进步和行业发展、以及保障社会公共信息体系的安全都具有极其重要的意义。

2. 标准编制技术路线

标准编制总体技术路线如下：

首先，本标准作为《测评要求》在大数据应用领域的扩展，总体架构沿袭《测评要求》。

其次，调研国内外大数据系统技术方案，研究提出符合实际需求的适用于大数据系统的细化的测评实施方法，以便更好指导测评机构开展相关工作。

再次，针对T/ISEAA 002-2021《信息安全技术 大数据安全等级保护基本要求》中各条款，提出具体测评实施方法。

3. 解决的主要问题

本标准适用于运营者依据《网络安全法》及《信息安全等级保护管理办法》，委托等级保护测评认证机构对大数据等级保护对象开展等级保护测评，主要解决以下问题：

- （1）明确大数据系统调研时的关注点；
- （2）确定大数据系统的具体测评对象以及测评实施关注点；
- （3）针对每条扩展安全要求的具体测评实施方法。

4. 标准文本架构

本标准共分为8章，3个附录，每章内容如下：

第1、2、3章，为标准的常规性描述，包括范围、规范性引用文件、术语和定义；

第4章，概要描述了大数据等级保护对象的含义，系统调研、测评对象确定、测评指标确定以及测评实施等各方面需要特殊关注的关注点；

第5、6、7、8章，分别描述了第二级到第五级的安全测评要求。主要针对 T/ISEAA 002-2021《信息安全技术 大数据安全等级保护基本要求》中的每一条款明确了具体的测评实施方法。

附录A，描述了测评单元的编号说明。

附录B，描述了不同展现形态的大数据等级保护对象与安全要求的映射关系。

附录C，描述了T/ISEAA 002-2021中条款可能涉及的高风险判例场景。

三、产业化情况、推广应用论证和预期达到的经济效果

本标准将推动大数据安全保护工作在各行业的落地实施，用于指导第三方测评机构规范化开展大数据安全测评工作，提升大数据等级保护对象的安全防护能力。

四、与现行相关法律、法规、规章及相关标准的协调性

本标准与现行法律、法规以及国家标准没有冲突与矛盾的地方。

与本标准配套使用的主要标准是 T/ISEAA 002-2021《信息安全技术 大数据安全等级保护基本要求》以及 GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》。

五、重大分歧意见的处理经过和依据

项目组在标准编制过程中，经历了内部讨论与论证、专家评审等过程，项目组在工作过程中遵循编制原则，对国内外现状做了大量调研，完成了标准修订工作。

本标准编制过程中，如标准编制组内部出现重大意见分歧时，由标准编制组组长组织召开内部调解会解决；如标准编制单位之间出现重大意见分歧，由标准编制承担单位公安部信息安全等级保护评估中心组织召开参编单位调解会解决。如征求意见过程中，各厂家，特别是各部委意见与标准编制组之间出现重大意见

分歧，由中关村信息安全测评联盟组织召开协调会解决，并认真听取专家意见进行修改。

在整个过程中对专家提出的意见和建议，我们做了应答和处理，更好地完善了我们的标准编制工作。

六、标准性质的建议

建议本标准是推荐性标准。

七、贯彻标准的要求和措施建议

本标准为开展大数据等级保护对象网络安全等级测评提供实施方法指导，建议在全国测评机构中推荐性实施。

八、替代或废止现行相关标准的建议

无。

九、其它应予说明的事项

1. 名称更改说明

目前，大数据等级保护对象的定义非常明确，因此建议将《信息安全技术 大数据安全等级保护定级及测评工作指南》改名为《网络安全等级保护大数据测评指南》。

《网络安全等级保护大数据测评指南》编制工作组

2023-04-10