团体标准《计算机信息系统安全服务规范》编制说明

一、 工作简况

1.1 任务来源

《计算机信息系统安全服务规范》由北京网络空间安全协会、广东省网络空间安全协会归口管理。

1.2 主要起草单位和工作组成员

本标准由网安联认证中心牵头，广州电力设计院有限公司、国源天顺科技产业集团有限公司、广东关键信息基础设施保护中心、广东新兴国家网络安全和信息化发展研究院、广州华南检验检测中心有限公司等多家单位共同参与编制。

1.3 主要工作过程

（1）2023 年 10 月，标准正式立项；

（2）2023 年 11-12 月，组织参与本标准编写的人员召开项目启动会，成立规范编制小组，确立各自分工，进行初步设计，并听取各参与单位的相关意见；

（3）2024 年 1-3 月，编制组召开组内研讨会并结合充分的调研结果，参考各类国家标准和相关政策文件，形成标准草案第一稿，后期经内部深入讨论研究，形成第二稿；

（4）2024 年 4 月，编制组继续召开组内研讨会，基于前期成果，经多次内部讨论研究，进一步对草案进行认真修改完善，形成征求意见稿。

二、标准编制原则和标准编制详细说明及解决的主要问题

2.1 编制原则

本标准的研究与编制工作遵循以下原则：

（1）符合性原则

本标准使用时能够与法律法规和国家强制性标准的要求保持一致，符合国家相关主管部门的要求。

（2）实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变的同时，针对需求群体，做到可操作、可用与实用。

2.2 文档结构

《计算机信息系统安全服务规范》标准文档分为前言、引言、范围、规范性引用文件、术语和定义、安全服务机构等级划分、安全服务机构评定标准、安全服务机构基本能力要求、安全服务机构分级能力要求、安全服务机构服务能力过程要求、评定方法等部分。

2.3 整体格式

整体格式根据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》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总过程中，对各编写组成员提交部分，根据GB/T 1.1-2020的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

2.4 标准名称英文翻译

标准的名称“计算机信息系统安全服务规范”翻译为Specification for security services of computer information system。

2.5 术语和定义

术语和定义中所列的术语的英文翻译，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

2.6 安全服务机构等级划分

本章阐述了安全服务机构等级的划分，依据安全服务机构的基本条件、基本资格、管理能力、技术服务能力等分为一级、二级、三级、四级，其中一级最高，四级最低。

2.7 安全服务机构评定标准

本章主要介绍了安全服务机构等级评定要求包含基本能力要求、分级能力要求和服务能力过程要求。

2.8 安全服务机构基本能力要求

本章介绍了安全服务机构应具备的基本条件包括具有中华人民共和国境内注册的独立法人资格，并具有相关部门颁发的合法经营资格；拥有长期固定的办公场所，具有能满足业务需求的设备和环境；遵守国家现行法律、法规，无违法记录等条件。

安全服务机构应具备的基本管理能力包括建立人员管理制度和能力考核指标，制定相关培训计划，定期开展培训；建立文档管理制

度，确保项目文档资料妥善保管；建立质量管理制度，跟踪服务质量，并能对服务质量进行持续改进等。

安全服务机构应具备的基本技术能力包括具备评估系统安全威胁的能力、评估系统脆弱性的能力、评估安全对系统的影响的能力、评估系统安全风险的能力、确定系统安全需求的能力、确定系统的安全输入的能力、安全控制管理的能力、监测系统安全状况的能力、检测或证实系统安全性的能力、建立系统安全的保证数据的能力以及对整个系统进行管理配置的能力。

2.9 安全服务机构分级能力要求

本章主要阐述了分级能力要求为安全服务机构各级别的能力要求，包含基本资格、管理能力要求、技术能力要求。

2.10 安全服务机构服务能力过程要求

本章介绍了安全服务机构应具备的服务能力过程要求，包括制定安全服务流程；制定安全服务规范，按照规范实施；服务过程至少包含准备阶段、设计阶段、实施阶段、服务保障阶段。

2.11 评定方法

本章介绍了第三方评审机构按公开、公正、公平原则，定性与定量相结合原则，实行统一标准、统一程序、统一管理原则开展评定工作。对安全服务机构等级评定采取文档审核、现场审核、综合评定的模式进行。

三、知识产权情况说明

本标准不涉及专利。

四、采用国际标准和国外先进标准情况

无采用国际标准和国外先进标准情况。

五、与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐性实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

六、重大分歧意见的处理经过和依据

《计算机信息系统安全服务规范》编制过程中未出现重大分歧。

七、标准性质的建议

建议《计算机信息系统安全服务规范》作为推荐性团体标准发布实施。

八、贯彻标准的要求和措施建议

鉴于本标准是规范计算机信息系统安全服务标准，适用于第三方评审机构对在从事计算机信息系统安全服务的机构进行等级评定，评定结果可作为政府部门和企事业单位选用安全服务时的参考依据；也可作为从事计算机信息系统安全服务的机构改进自身服务能力的指导。按照标准要求实施计算机信息系统安全服务机构等级评定，客观公正地评价服务机构的服务能力，既可作为服务机构开展自我评价的规范和标准，也可为行业监管、用户在维护计算机信息系统安全工作中选择服务机构提供依据，有利于规范市场秩序、杜绝不良企业涉足计算机信息系统安全行业，促进计算机信息系统安全服务行业的健康发展，切实保护我国的信息安全、网络安全和数据安全。

九、替代或废止现行相关标准的建议

无替代或废止。

十、其他应予说明的事项

无。

《计算机信息系统安全服务规范》标准编制组

2024 年 4 月