团体标准《电子政务系统商密应用安全性评估中数据安全测评规范》编制说明

一、 工作简况

1.1 任务来源

《电子政务系统商密应用安全性评估中数据安全测评规范》由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

本标准由华南师范大学、数字广东网络建设有限公司牵头，工业和信息化部电子第五研究所、深圳奥联信息安全技术有限公司、广州竞远安全技术股份有限公司、广东申腾信息技术有限公司、华南农业大学、北京海泰方圆科技股份有限公司等多家单位共同参与编制。

1.3 主要工作过程

（1）2022 年 11 月，标准正式立项，广东省网络空间安全协会发布《电子政务系统密码测评中数据安全评估规范》团体标准立项公告；

（2）2022 年 12 月-2023 年 4 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，对电子政务系统商用密码测评工作进行调研，走访多家测评服务单位，听取各单位的相关意见；

（3）2023 年 5 月-2023 年 7 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；

（4）2023 年 8 月-2023 年 9 月，编制组召开组内研讨会,结合各参编单位的反馈意见，修改形成标准草案第二稿；结合国家密码管理局《商用密码应用安全性评估管理办法》，编制组决定将本团体标准的名称更改为《电子政务系统商密应用安全性评估中数据安全测评规范》；

（5）2023 年 10 月-2023 年 11 月，编制组召开组内研讨会，基于前期成果，经多次内部讨论研究，组织完善草案内容，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，针对服务群体，做到可操作、可用与实用。

2.2 文档结构

《电子政务系统商密应用安全性评估中数据安全测评规范》标准文档分为前言、引言、范围、规范性引用文件、术语和定义、缩略语、

电子政务系统商密应用安全性评估中数据安全总体框架、电子政务系统商密应用安全性评估中数据生命周期安全防护要求、电子政务系统密码应用中数据安全管理要求、电子政务商密应用安全性评估中数据安全测评规范、附录等部分。

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。

在标准内容汇总及整个各方意见过程中，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“电子政务系统商密应用安全性评估中数据安全测评规范” 翻译为The specification of data security assessment for commercial cryptography application security evaluation in E-governance systems。

结合国家密码管理局审议通过《商用密码应用安全性评估管理办法》，编制组将本团体标准更名为《电子政务系统商密应用安全性评估中数据安全测评规范》（原名称为《电子政务系统密码测评中数据安全评估规范》），以与管理办法的表述保持一致。

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 电子政务系统商密应用安全性评估中数据安全总体框架

本章主要阐述了电子政务系统商密应用安全性评估中数据安全总体框架，包括数据安全保障能力，数据安全密码应用能力，以及电子政务系统数据生命周期中的安全保障能力。数据安全保障能力应实施电子政务系统的数据分类分级管理，建立组织保障制度和运维保障规范，通过数据安全评估提升数据安全的保障能力。数据安全密码应用能力应重点实现数据的机密性、完整性、真实性、敏感性，降低数据破坏、泄漏的风险。

2.7电子政务系统商密应用安全性评估中数据生命周期安全防护要求

本章主要介绍了数据采集、数据传输、数据存储、数据处理、数据交换以及数据清除等阶段的安全防护要求。数据采集存在数据源伪造、特权账户滥用、数据泄露、数据篡改、恶意数据注入等安全风险，应基于商用密码技术保障数据来源的真实性，保障采集安全级别3级以上数据的机密性与完整性。数据传输存在数据篡改、伪造及窃取等安全风险，应基于商用密码技术保障数据在传输过程中的机密性、完整性、真实性。数据存储存在数据泄露、数据篡改等安全风险，应基于密码技术保障数据存储过程中的机密性、完整性。数据处理存在越权访问、数据篡改等安全风险，应基于密码技术保障数据处理的完整性、真实性、敏感性。数据交换存在数据泄露、数据篡改等安全风险，

应基于密码技术保障数据交换的机密性、完整性、真实性、敏感性。数据清除存在因数据恢复而泄露的安全风险，应基于密码技术保障数据的机密性。

2.8 电子政务系统密码应用中数据安全管理要求

本章分别介绍了电子政务系统密码应用中数据安全管理要求，明确了管理制度、人员管理、权限管理、建设运行、日志存留、安全审计、应急处置等方面的相关管理要求。

2.9 电子政务商密应用安全性评估中数据安全测评规范

本章介绍电子政务系统商密应用安全性评估中数据安全测评规范。主要利用人员访谈、文件审查、配置检查及测试验证等多种方法评估开展商密应用安全性评估后的电子政务系统在各类数据处理活动及数据承载系统平台的保障措施合规情况，从通用性管理与全生命周期管理两方面出发，针对各个指标项明确评估涉及的重要管理措施、重点技术措施及判断标准，明确被评估事项合规性保障基线，以提升数据安全管理及相关技术保障措施能力水平。

数据安全评估应遵循标准性原则、客观公正原则、可重复和可再现原则、可控性原则、完备性原则、最小影响原则以及保密原则。重点对评估流程中的评估实施规范进行说明，并介绍了评估报告的规范要求。

三、知识产权情况说明

本标准的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

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

《电子政务系统商密应用安全性评估中数据安全测评规范》编制过程中未出现重大分歧。

七、标准性质的建议

建议《电子政务系统商密应用安全性评估中数据安全测评规范》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

建议商用密码应用单位以及测评服务单位按规范贯彻执行商用密码应用安全性评估，推动商用密码应用落地，确保电子政务系统数据安全。

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。

《电子政务系统商密应用安全性评估中数据安全测评规范》

标准编制组

2023 年 11 月