团体标准《重要信息基础设施供应链安全检查评估规范》编制说明

一、 工作简况

1.1 任务来源

《重要信息基础设施供应链安全检查评估规范》由广东关键信息基础设施保护中心作为提出单位。该标准由北京网络空间安全协会和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

本标准由广东关键信息基础设施保护中心牵头，网安联认证中心有限公司、广东新兴国家网络安全和信息化发展研究院等多家单位共同参与编制。

1.3 主要工作过程

（1）2022 年 1-3 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，并听取各协作单位的相关意见。

（2）2022 年 4-5 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，后期经内部多次讨论研究，形成第二稿。

（3）2022 年 5 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

本标准符合法律法规和强制性标准要求,不损害人身健康和生命财产安全、国家安全、生态环境安全，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，针对不同的用户群体，做到可操作、可用与实用。

2.2 文档结构

《重要信息基础设施供应链安全检查评估规范》标准文档分为前言、范围、规范性引用文件、术语和定义、检查评估的依据与原则、评估流程、现场评估方法、评估内容与服务输出等部分。

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过来的部分，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“重要信息基础设施供应链安全检查评估规范”翻译

为 Specification for security inspection and evaluation of important information infrastructure supply chain。

2.5 术语和定义

术语和定义中所列的术语的英文翻译，根据各部分编写成员提供的术语，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 评估依据与原则

本章主要阐述了重要信息基础设施供应链安全检查评估的依据与原则，评估依据包括遵循网络安全、网络安全审查相关法律法规，依照相关要求及标准规范等；评估原则遵循标准性原则、 规范性原则、 完整性原则、保密性原则和最小影响原则。

2.7 安全检查评估流程

本章介绍了重要信息基础设施供应链安全检查评估的评估范围、目的和实施流程。

安全检查的评估范围是基于重要信息基础设施开展网络产品和服务全生命周期评估，从产品测评、产品认证、供应商评估、安全审查等多项措施强化供应链安全管理。

安全检查的评估旨在帮助企业了解其供应商，发现可能的第三方风险及自身管理缺陷问题，并提出相应的整改建议，加强供应链安全管理，防范供应链风险。

安全检查评估流程首先需进行前期沟通与资料收集，做好评估前

的坏境准备等工作。然后进行现场评估，包括技术检测和管理评估两个方面。根据现场评估情况对产品安全技术检测和安全管理自查结果梳理，整理风险点列表，出具相关报告。

最后会为企业提供协助整改与监督检查支持帮助。

2.8 现场评估方法

本章分别介绍了现场评估的方法，现场评估方法包括使用代码审计、漏洞扫描、渗透测试和软件安全分析来对产品安全技术进行检测；使用问卷调查、文档审查、业务参与与风险梳理、人员访谈和控制措施有效性验证来进行管理评估。

2.9 评估内容与服务输出

本章介绍了评估内容与服务输出结果。评估内容包含产品安全技术检测和管理评估，产品安全技术检测主要内容包括对产品的销售许可证及其第三方安全检测的检查以及产品技术风险点检测。管理评估主要内容主要包括组织管理、流程与政策、供应商管理、人员管理、产品漏洞管理、源代码安全管理、产品安全开发管理、统一安全管理等。

服务输出结果包括项目实施计划、重要信息基础设施供应链产品安全技术评估报告、重要信息基础设施供应链管理能力风险评估报告和重要信息基础设施供应链安全评估问题清单等。

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

《重要信息基础设施供应链安全检查评估规范》编制过程中未出现重大分歧。

七、标准性质的建议

建议《重要信息基础设施供应链安全检查评估规范》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

鉴于本标准是重要信息基础设施供应链安全检查评估规范标准，用于指导重要信息基础设施供应链安全检查评估工作、适用重要信息基础设施运营单位开展重要信息基础设施供应链安全自查评估，建议在标准贯彻执行过程中，各单位应当起到协调以及推广的作用。

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。

《重要信息基础设施供应链安全检查评估规范》标准编制组

2022 年 5 月