团体标准《重要信息系统终端防范高级持续性威胁安全检查指南》编制说明

一、 工作简况

1.1 任务来源

《重要信息系统终端防范高级持续性威胁安全检查指南》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，广东电网有限责任公司信息中心、安芯网盾（北京）科技有限公司、深圳供电局有限公司、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）2021 年 9-10 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）2021 年 11-12 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 1-2 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

《重要信息系统终端防范高级持续性威胁安全检查指南》标准文档分为前言、范围、规范性引用文件、术语和定义、检查方式、检查工作实施流程、检查内容的选择方法和检查内容等部分。

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“重要信息系统终端防范高级持续性威胁安全检查指南”翻译为 Guide for security inspection of important information system terminals against advanced persistent threats。

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 检查方式

本章主要阐述了重要信息系统终端防范高级持续性威胁安全检查方式，分别为监督检查、自检查以及委托检查。

2.7 检查工作实施流程

本章包括重要信息系统终端防范高级持续性威胁安全检查工作的实施流程内容。

计划准备阶段，明确检查工作的要求、依据、范围、内容、安全检查工作计划、工作方案等内容；明确工作职责，包括检查机构向被检查单位介绍安全检查的相关情况、准备安全检查所需材料和确定人员等；被检查机构向检查机构提供本单位基本情况介绍、提供办公条件、做好数据备份以及制定应急预案等。

现场检查阶段，检查机构调研检查被检查单位的资产范围、向被检查单位说明检查的工作步骤和工作方法及实施现场检查工作；被检

查机构协调配合检查的内部相关人员关系，有序开展受检工作。

现场检查阶段工作完成后，由检查组对检查结果进行整理并分析上报。

隐患整改阶段，运营单位内部的网络安全责任单位汇总检查结果、分析问题隐患、研究整改措施以及最后编写总结报告。

2.8 检查内容的选择方法

本章分别介绍了全覆盖法、重点项抽取法以及增项检查法等检查内容的选择方法。

2.9 检查内容

本章介绍了检查内容主要是对终端安全的防范检查，包括终端品牌、操作系统，终端安全软件情况的检查，主要涉及入侵防范、恶意代码防范、威胁检测与防御、可信验证、身份鉴别、访问控制、安全审计及数据完整性等方面。

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

《重要信息系统终端防范高级持续性威胁安全检查指南》编制过

程中未出现重大分歧。

七、标准性质的建议

建议《重要信息系统终端防范高级持续性威胁安全检查指南》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系统终端防范高级持续性威胁安全检查指南标准，用于指导重要信息系统终端防范高级持续性威胁安全监督检查、委托检查工作以及自检查，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。

《重要信息系统终端防范高级持续性威胁安全检查指南》标准编制组

2022 年 3 月