ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35280—2017

信息安全技术　信息技术产品安全检测机构条件和行为准则

Information security technology—Requirement and code of conduct for security testing bodies of information technology products

2017-12-29 发布　　2018-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国电子技术标准化研究院、中国信息安全测评中心、中国信息安全研究院有限公司、北京信息安全测评中心、国家信息技术安全研究中心、公安部第三研究所、国家保密科技测评中心、国家应用软件产品质量监督检验中心、中国信息安全认证中心、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、中国科学院软件研究所、陕西省网络与信息安全测评中心、西安电子科技大学、重庆邮电大学、华东师范大学、国网江苏省电力公司电力科学研究院。

本标准主要起草人:范科峰、王惠莅、龚洁中、李琳、任泽君、王春佳、杨晨、顾健、杨宏宁、王坤、董晶晶、李凤娟、张宝峰、时志伟、魏方方、甘杰夫、刘玉岭、贺海、马文平、杨帆、裴庆琪、杨力、黄永洪、何道敬、刘虹、黄伟。

引　言

为保障关键信息基础设施网络安全，消减因为大量使用的信息技术产品可能给设施引入的安全缺陷、漏洞、恶意程序等潜在的安全风险，需要通过对信息技术产品安全检测，提高信息技术产品供应方产品的安全保障能力。

同时为加强信息技术产品安全检测机构管理，规范信息技术产品安全检测机构行为，保障检测活动的公正可信性以及安全检测机构的能力水平，促使信息技术产品供应方提高产品的安全保障能力，保障国家关键信息基础设施安全，制定本标准。

信息安全技术　信息技术产品安全检测机构条件和行为准则

1　范围

本标准规定了信息技术产品安全检测机构应具备的条件以及应遵守的行为准则。

本标准适用于从事信息技术产品安全性检测的第三方机构，可为相关主管部门、信息技术产品供应方和用户选择第三方检测机构提供参考。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010　信息安全技术　术语

GB/T 27000—2006　合格评定　词汇和通用原则

GB/T 27025　检测和校准实验室能力的通用要求

GB/T 32921—2016　信息安全技术　信息技术产品供应方行为安全准则

3　术语和定义

GB/T 25069—2010、GB/T 27000—2006 和 GB/T 32921—2016 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了 GB/T 32921—2016 中的一些术语和定义。

3.1

信息技术产品　information technology product

具有采集、存储、处理、传输、控制、交换、显示数据或信息功能的硬件、软件、系统和服务。

注：信息技术产品包括计算机及其辅助设备、通信设备、网络设备、自动控制设备、操作系统、数据库、应用软件与服务等。

[GB/T 32921—2016，定义 3.1]

3.2

信息技术产品供应方　information technology product supplier

提供信息技术产品的组织。

注：信息技术产品供应方包括生产商、销售商、代理商、集成商、服务商等。

[GB/T 32921—2016，定义 3.2]

3.3

信息技术产品安全检测机构　security testing bodies of information technology products

从事信息技术产品安全检测活动的第三方机构。

注 1：信息技术产品安全检测机构可以是一个组织，或是一个组织的一部分。

注 2：本标准中信息技术产品安全检测机构简称“检测机构”。