ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28449—2012

信息安全技术
信息系统安全等级保护测评过程指南

Information security technology—Testing and evaluation process guide for classified protection of information system security

2012-06-29 发布　　2012-10-01 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:公安部信息安全等级保护评估中心。

本标准主要起草人:袁静、任卫红、陈雪秀、曲洁、刘静、毕马宁、朱建平、马力、李明、李升、黄洪。

引　言

依据《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)、《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号),制定本标准。

本标准是信息安全等级保护相关系列标准之一。

与本标准相关的系列标准包括:

——GB/T 22239—2008　信息安全技术　信息系统安全等级保护基本要求;

——GB/T 22240—2008　信息安全技术　信息系统安全等级保护定级指南;

——GB/T 28448—2012　信息安全技术　信息系统安全等级保护测评要求。

信息安全技术
信息系统安全等级保护测评过程指南

1 范围

本标准规定了信息系统安全等级保护测评(以下简称“等级测评”)工作的测评过程,对等级测评的活动、工作任务以及每项任务的输入/输出产品等提出指导性建议。

本标准适用于测评机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评价。

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 5271.8 信息技术 词汇 第8部分:安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求

《信息安全等级保护管理办法》(公通字[2007]43号)

3 术语和定义

GB/T 5271.8、GB 17859—1999 和 GB/T 28448—2012 界定的以及下列的术语和定义适用于本文件。

3.1

优势证据 superior evidence

测评结果显现的凭据强于其他测评结果的那个/些测评结果视为优势证据。它可用于平衡实施等级测评过程中获得的多个测评结果之间的矛盾。

4 符号和缩略语

DDN:数字数据网 (Digital Data Network)

PSTN:公共交换电话网络 (Public Switched Telephone Network)

SDH:同步数字体系 (Synchronous Digital Hierarchy)

5 等级测评概述

5.1 等级测评的作用

依据《信息安全等级保护管理办法》(公通字[2007]43号),信息系统运营、使用单位在进行信息系