

NIST 特别出版物 800-55

第 I 修订版 (草案)

**NIST**

**National Institute of  
Standards and Technology**

Technology Administration  
U.S. Department of Commerce

**信息安全绩效**

**测量指南 (草案)**

Elizabeth Chew  
Marianne Swanson  
Kevin Stine  
Nadya Bartol  
Anthony Brown

**信息安全**

国家标准和技术研究所  
信息技术实验室  
计算机安全处

Gaithersburg, MD 20899-8930

2007 年 9 月



美国商务部

部长: *Carlos M. Gutierrez*

国家标准和技术研究所

代理主任: *James M. Turner*

# 目录

## 执行摘要

### 1. 概述

- 1.1 目的和适用范围
- 1.2 适用对象
- 1.3 历史
- 1.4 成功的关键因素
- 1.5 与其他 NIST 文件的关系
- 1.6 本文的篇章结构

### 2. 角色和责任

- 2.1 机构领导
- 2.2 首席信息官
- 2.3 机构高级信息安全官
- 2.4 项目经理 / 信息系统拥有者
- 2.5 信息系统安全官
- 2.6 其他相关角色

### 3. 信息安全测量的背景信息

- 3.1 定义
- 3.2 使用测量的益处
- 3.3 测量的类型
  - 3.3.1 执行测量
  - 3.3.2 有效性 / 效果测量
  - 3.3.3 影响测量
- 3.4 测量时应该考虑的因素
  - 3.4.1 机构因素
  - 3.4.2 可管理性
  - 3.4.3 数据管理因素
  - 3.4.4 测量数据收集的自动化
- 3.5 风险管理框架内的测量
- 3.6 信息安全测量方案的适用范围
  - 3.6.1 单个信息系统
  - 3.6.2 系统开发生命周期
  - 3.6.3 面向整个企业的方案

### 4. 立法和战略驱动

- 4.1 立法因素
  - 4.1.1 政府绩效和结果法案
  - 4.1.2 联邦信息安全管理法案
- 4.2 其他行政部门提案
- 4.3 企业战略规划与信息安全的衔接

### 5. 测量开发流程

- 5.1 利益相关人及其兴趣的确定
- 5.2 目的和目标定义

- 5.3 信息安全策略、指南和规程查阅
- 5.4 信息安全方案执行查阅
- 5.5 测量的开发和选择
  - 5.5.1 测量开发的方法
  - 5.5.2 测量的重点安排和选择
  - 5.5.3 建立绩效目标
- 5.6 测量开发模板
- 5.7 测量开发流程内的反馈
- 6. 信息安全测量的执行**
  - 6.1 准备收集数据
  - 6.2 收集数据和分析结果
  - 6.3 确定纠正行动
  - 6.4 建立业务个案和获得资源
  - 6.5 实施纠正行动
- 附录 A 备用测量方法**
- 附录 B 缩略语**
- 附录 C 参考文献**
- 附录 D 最低安全要求说明**