

NIST 特别出版物 800-100

征求意见稿

**NIST**

**National Institute of  
Standards and Technology**

Technology Administration  
U.S. Department of Commerce

**信息安全手册:**

**经理指南**

**国家标准和技术研究所的建议**

Pauline Bowen

Joan Hash

Mark Wilson

Nadya Bartol

Gina Jamaldinian

## 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

2006 年 6 月



美国商务部

部长: *Carlos M. Gutierrez*

技术局

商务部技术副部长: *Robert Cresanti*

国家标准和技术研究所

主任: *William Jeffrey*

# 目录

## 第1章 概述

- 1.1 目的和适用范围
- 1.2 与现行指南的关系
- 1.3 适用对象

## 第2章 信息安全监管

- 2.1 信息安全监管要求
- 2.2 信息安全监管构成
  - 2.2.1 信息安全战略规划
  - 2.2.2 信息安全监管体系
  - 2.2.3 监管的关键角色和责任
    - 2.2.3.1 机构领导
    - 2.2.3.2 首席信息官
    - 2.2.3.3 高级信息安全官
    - 2.2.3.4 首席构架师
    - 2.2.3.5 其他相关角色
  - 2.2.4 联邦政府组织构架
  - 2.2.5 信息安全政策和指南
  - 2.2.6 持续监控
- 2.3 信息安全监管的挑战和成功关键

## 第3章 系统开发生命周期

- 3.1 启动阶段
- 3.2 开发 / 采购阶段
- 3.3 执行阶段
- 3.4 运行 / 维护阶段
- 3.5 处置阶段
- 3.6 系统开发生命周期中的安全活动

## 第4章 意识培养和培训

- 4.1 意识培养和培训政策
- 4.2 组成：意识培养、培训、教育和认证
  - 4.2.1 意识培养
  - 4.2.2 培训
  - 4.2.3 教育
  - 4.2.4 认证
- 4.3 设计、开发和落实意识培养和培训项目
  - 4.3.1 设计意识培养和培训项目
  - 4.3.2 开发意识培养和培训项目
  - 4.3.3 落实意识培养和培训项目
- 4.4 后续行动
  - 4.4.1 监督遵规
  - 4.4.2 评价和反馈
- 4.5 变动管理

- 4.6 项目的成功指标
- 第5章 资本规划
  - 5.1 立法综述
  - 5.2 资本规划的角色和责任
  - 5.3 确定基线
  - 5.4 优先顺序排列准则
  - 5.5 进行系统层面和组织层面的优先顺序排列
  - 5.6 编制支持材料
  - 5.7 IRB 和投资组合管理
  - 5.8 Exhibit 53 和 300 及项目管理
- 第6章 互联系统
  - 6.1 管理系统互联
  - 6.2 生命周期管理法
    - 6.2.1 第一阶段：计划互联
    - 6.2.2 第二阶段：建立互联
    - 6.2.3 第三阶段：维护互联
    - 6.2.4 第四阶段：切断互联
  - 6.3 终止互联
    - 6.3.1 紧急切断
    - 6.3.2 恢复互联
- 第7章 绩效度量
  - 7.1 测度类型
  - 7.2 测度的开发和实施方法
  - 7.3 测度的开发过程
  - 7.4 测度方案实施
    - 7.4.1 准备收集数据
    - 7.4.2 收集数据和分析结果
    - 7.4.3 确定纠正行动
    - 7.4.4 开发业务案例和获得资源
    - 7.4.5 实施纠正行动
- 第8章 安全计划
  - 8.1 主要应用、通用支持系统和次要应用
  - 8.2 安全计划的角色和责任
    - 8.2.1 首席信息官
    - 8.2.2 信息系统拥有者
    - 8.2.3 信息拥有者
    - 8.2.4 高级信息安全官
    - 8.2.5 信息系统安全官
  - 8.3 行为准则
  - 8.4 系统安全计划的审批
    - 8.4.1 系统边界分析和安全控制
    - 8.4.2 安全控制
    - 8.4.3 适用范围指南

- 8.4.4 补偿性控制
- 8.4.5 通用安全控制
- 8.5 安全控制选择
- 8.6 完成和批准日期
- 8.7 持续的系统安全计划维护
- 第9章 信息技术应急规划
  - 9.1 第一步：制定应急规划政策
  - 9.2 第二步：进行业务影响分析
  - 9.3 第三步：确定预防性控制
  - 9.4 第四步：制定恢复战略
  - 9.5 第五步：制定 IT 应急计划
  - 9.6 第六步：计划测试、培训和演练
  - 9.7 计划维护
- 第10章 风险管理
  - 10.1 风险评价
    - 10.1.1 第一步——系统特性描述
    - 10.1.2 第二步——威胁识别
    - 10.1.3 第三步——脆弱性识别
    - 10.1.4 第四步——风险分析
      - 10.1.4.1 控制分析
      - 10.1.4.2 可能性确定
      - 10.1.4.3 影响分析
      - 10.1.4.4 风险确定
    - 10.1.5 第五步——控制建议
    - 10.1.6 第六步——结果记录归档
  - 10.2 风险缓释
  - 10.3 评估和评价
- 第11章 认证、认可和安全评价
  - 11.1 认证、认可和安全评价的角色和责任
    - 11.1.1 首席信息官
    - 11.1.2 授权官员
    - 11.1.3 高级信息安全官
    - 11.1.4 信息系统所有者
    - 11.1.5 信息所有者
    - 11.1.6 信息系统安全官
    - 11.1.7 认证主体
    - 11.1.8 用户代表
  - 11.2 角色的授予
  - 11.3 安全认证和认可过程
  - 11.4 安全认证文件归档
  - 11.5 认可决定
  - 11.6 持续监控
  - 11.7 项目评价

- 第 12 章 安全服务和产品采购
  - 12.1 信息安全服务生命周期
  - 12.2 选择信息安全服务
    - 12.2.1 选择信息安全服务管理工具
    - 12.2.2 信息安全服务问题
    - 12.2.3 信息安全服务的总体考虑因素
  - 12.3 挑选信息安全产品
  - 12.4 IT 产品的安全检查列表
  - 12.5 机构利益冲突
- 第 13 章 事故响应
  - 13.1 准备
    - 13.1.1 事故响应准备
    - 13.1.2 收集事故数据准备
    - 13.1.3 预防事故
  - 13.2 检测和分析
  - 13.3 遏制、根除和恢复
  - 13.4 后续活动
- 第 14 章 配置管理
  - 14.1 系统开发生命周期中的配置管理
  - 14.2 配置管理的角色和责任
  - 14.3 配置管理进程
- 附录 B 常见问题解答

