

NIST 特别出版物 800-53  
第 5 版

# 信息系统和机构的 安全和隐私控制

(公开征求意见稿初版)

内部资料

高卓翻译

联合任务组

本出版物包含了技术和非技术安全和隐私控制的完整目录。这些控制可以支持各种专业应用，其中包括用于开发系统、产品、组件和服务以及用于保护机构、系统和个人的“风险管理框架”、“网络安全框架”和“系统工程流程”。

国家标准和技术研究所  
信息技术实验室  
计算机安全部  
2017 年 8 月



美国商务部  
Wilbur L. Ross, Jr., 理部长  
国家标准和技术研究所  
Kent Rochford, 负责标准和技术的商务部副部长  
兼NIST代所长

**NIST**  
国家标准和技术研究所  
美国商务部

北京江南天安科技有限公司

# 目录

## 第 1 章 概述

- 1.1 目的和适用范围
- 1.2 适用对象
- 1.3 机构的责任
- 1.4 与其他出版物的关系
- 1.5 修订和扩充
- 1.6 篇章结构

## 第 2 章 基本概念

- 2.1 要求和控制
- 2.2 控制的组织结构
- 2.3 控制的类型
- 2.4 安全和隐私控制的关系
- 2.5 控制基线
- 2.6 保障和可信度

## 第 3 章 控制

- 3.1 访问控制 (AC)
- 3.2 意识和培训 (AT)
- 3.3 审计和追责 (AU)
- 3.4 评价、授权和监测 (CA)
- 3.5 配置管理 (CM)
- 3.6 应急预案 (CP)
- 3.7 识别与认证 (IA)
- 3.8 个人参与 (IP)
- 3.9 事故响应 (IR)
- 3.10 维护 (MA)
- 3.11 介质保护 (MP)
- 3.12 隐私授权 (PA)
- 3.13 物理和环境保护 (PE)
- 3.14 规划 (PL)
- 3.15 方案管理 (PM)
- 3.16 人员安全 (PS)
- 3.17 风险评价 (RA)
- 3.18 系统和服务采购 (SA)
- 3.19 系统和通信保护 (SC)
- 3.20 系统和信息的完整性 (SI)

## 附录 A 参考文献

## 附录 B 术语表

## 附录 C 缩略语

## 附录 D 控制基线

- 附录 E 控制汇总
- 附录 F 整合后的隐私控制总览
- 附录 G 裁剪方面的考虑
- 附录 H 控制的关键词
- 附录 I 国际标准

