国家信息中心
State Information Center

政务终端安全核心配置规范国标研制情况介绍

国家信息中心 李新友

2011年10月

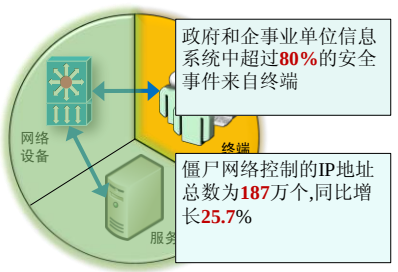
地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919

提 纲

- 立项背景
- 标准体系框架
- 应用支撑平台框架
- 标准工作进展情况

国家信息中心
State Information Center

终端安全受到普遍重视



政府和企事业单位信息系统中超过**80%**的安全事件来自终端

僵尸网络控制的IP地址总数为**187**万个,同比增长**25.7%**

国家信息中心
State Information Center

终端安全事件分析

1. 外部攻击

2. 系统存在漏洞

3. 终端安全配置不当

终端安全事件原因：

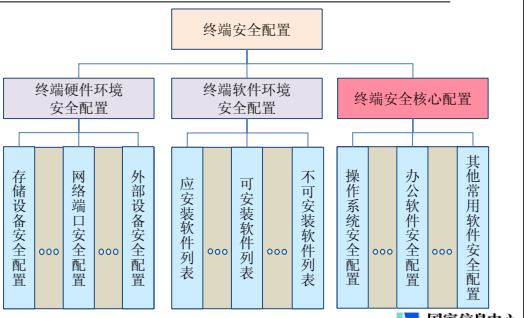
- **65%是配置不当**
- **30%是没有打补丁**
- **5%是零日漏洞**

终端安全保护方法：

- **定期杀毒**
- **及时打补丁**
- **正确配置**

国家信息中心
State Information Center

终端安全配置



国家信息中心 State Information Center

“终端安全核心配置”如何发挥作用

对操作系统、办公软件、浏览器等常用软件中关键的安全属性进行参数设置，限制或禁止存在安全隐患或漏洞的功能，启用或加强安全保护功能，增强终端抵抗安全风险的能力

- **禁止**
  - 高危服务和端口
  - 非法程序脚本执行
  - 未授权程序驱动安装
- **限制**
  - 用户权限
  - 程序内存配额
  - 远程进程调用(RPC)
- **加强**
  - 密码管理
  - 身份认证
  - 系统审核
- **启用**
  - 数字签名
  - 进程保护

6

国家信息中心 State Information Center

美国联邦政府桌面核心配置（FDCC）

- 2007年，美国联邦预算管理办公室（OMB）发布备忘录（M-07-11），开始实施FDCC
- FDCC强制规定,联邦政府所有Windows桌面终端必须进行安全配置，并对Windows XP, Vista, Windows 7，IE, Office的具体配置作出规定
- NIST制定SCAP标准支持FDCC自动化检查
- 2010年3月，美国联邦政府审计办公室（GAO）发布审计报告“政府机构必须实施桌面核心配置”

国家信息中心 State Information Center

我国加快终端安全配置标准立项工作

- CGDCC：政务终端安全核心配置
  China Government Desktop Core Configuration
  —— 2008年由国家信息中心正式提出
- 《政务终端安全核心配置规范》
  —— 2010年国标正式立项(计划号：20100392-T-469）
- “政务终端安全核心配置（CGDCC）标准研制及其验证、应用平台建设项目”
  —— 列入2010年国家高技术产业发展项目计划

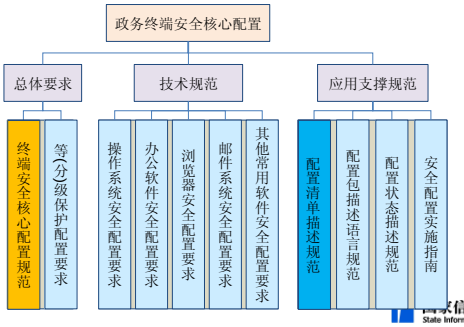
国家信息中心 State Information Center

提　纲

- 立项背景
- 标准体系框架
- 应用支撑平台框架
- 标准工作进展情况

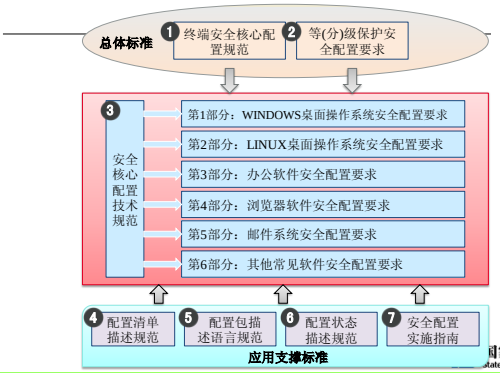
国家信息中心 State Information Center

CGDCC标准体系框架



国家信息中心 State Information Center

CGDCC标准之间的关系



国家信息中心 State Information Center

《政务终端安全核心配置规范》主要内容

- 本标准提出了政务终端安全核心配置的基本概念、总体技术和管理要求、应用支撑平台框架、以及实施流程。
- 总体技术要求：对操作系统和常用办公软件，从身份鉴别、访问控制、网络通信、资源管理、数据安全、安全审计等方面提出总体技术要求。
- 总体管理要求：从组织保障、文档要求和风险控制等方面提出总体管理要求。

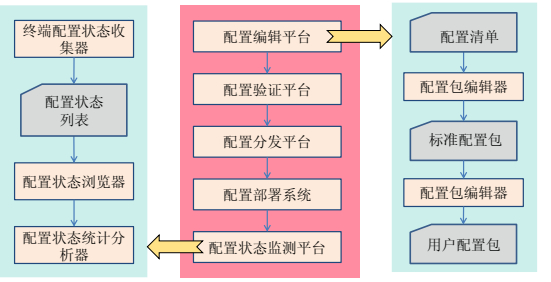
国家信息中心 State Information Center

《技术规范》研制课题分解情况

1	国产操作系统安全配置要求
2	国外非WINDOWS操作系统安全配置要求
3	IE浏览器安全配置要求
4	国外非IE浏览器安全配置要求
5	国产浏览器安全配置要求
6	国外办公软件安全配置要求
7	国产办公软件安全配置要求
8	国外邮件系统安全配置要求
9	国产邮件系统安全配置要求
10	下载与及时通信类常用软件安全配置要求
11	阅读、图片应用和媒体播放类常用软件安全配置要求
12	其他常用软件安全配置要求

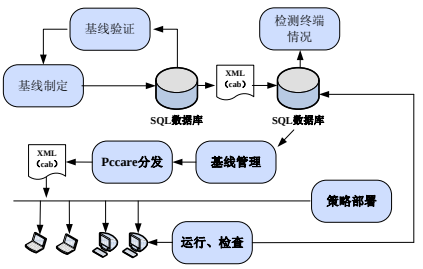
国家信息中心 State Information Center

《应用支撑规范》框架



国家信息中心 State Information Center

安全配置实施流程



国家信息中心 State Information Center

提　纲

- 立项背景
- 标准体系框架
- 应用支撑平台框架
- 标准工作进展情况

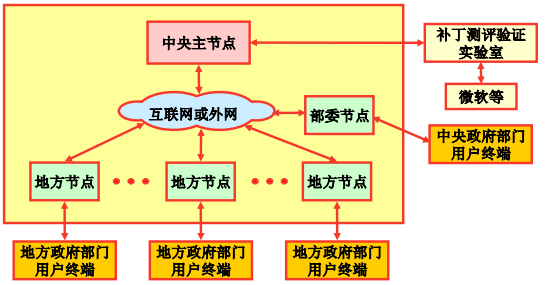
16

国家信息中心 State Information Center

应用支撑平台基本功能

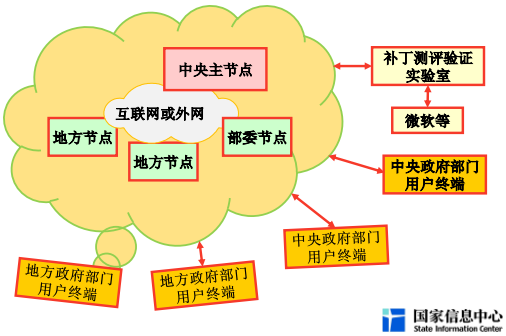
国家信息中心 State Information Center

应用支撑平台（PCcare)逻辑架构



国家信息中心 State Information Center

终端安全配置云服务平台的构想



国家信息中心 State Information Center

提　纲

- 立项背景
- 标准体系框架
- 应用支撑平台框架
- 标准工作进展情况

20

国家信息中心 State Information Center

标准研制进展

	标准名称	预研阶段	标准预编	国标编制
1	政务终端安全核心配置规范			
2	等级保护安全配置要求			
3	安全核心配置技术规范（6个部分）			
4	安全配置清单描述规范			
5	安全配置包描述语言规范			
6	安全配置状态描述规范			
7	政务终端安全核心配置实施指南			

国家信息中心 State Information Center

标准应用支撑平台建设进展

- 组织各地信息中心在全国范围内建设政务终端安全核心配置平台
  - 国家信息中心建设中央节点
  - 在24个省市信息中心建设地方节点
  - 在中国信息安全测评中心建设补丁测评实验室
  - 自主研制核心配置应用支撑软件 PCcare2011

配置工具开发进展

安全核心配置工具
✓ 配置基线管理
✓ 配置分发部署
✓ 配置状态监测
✓ 配置状态报告
✓ 配置检查（专用）
○ 配置包编辑器
○ 配置验证测试工具

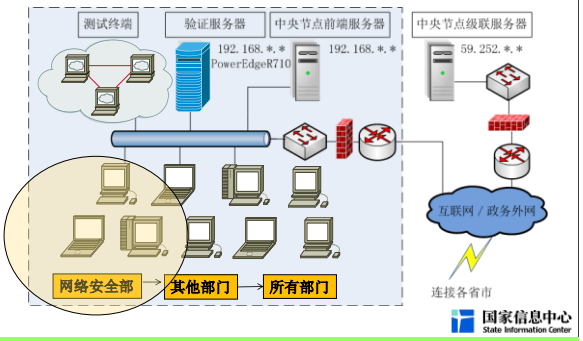
国家信息中心 State Information Center

标准示范应用情况

- 试点：
  - 四川、安徽
- 示范：两级平台
  - 国家信息中心：处室——部门——中心
  - 山西、四川、广西、山东等的发改委
  - 上海市物价系统

国家信息中心 State Information Center

国家信息中心示范应用情况



国家信息中心
State Information Center

示范应用效果

- 员工
  - 漏洞补丁及时更新
  - 系统得到正确配置，弥补个人原因造成的疏漏
- 单位领导
  - 掌握全网终端的安全状况和存在的安全问题
  - 安全策略统一部署提高安全措施的实施效率
  - 终端安全维护及检查工作量大为降低
- 国家安全主管部门
  - 可掌握全国政务终端的安全状况、安全事件发生趋势
  - 可了解病毒爆发情况，做到有效预防和有效控制
  - 可全面提高我国政务终端的整体安全性

国家信息中心
State Information Center

国家信息中心
State Information Center

谢 谢！

地址：北京市西城区三里河路58号 邮编：100045 电话：010-68527618 68557203 传真：010-68533919