电子政务的
安全态势与顶层设计

吴世忠

中国信息安全测评中心

2010年6月27日

北京大学

主 要 内 容

一、国外政府信息安全形势

二、我国电子政务安全环境

三、安全顶层设计工作建议

前　言

1、网络无处不在，安全不可或缺：全球共识。

2、漏洞隐患显现，安全风险调整：大势所趋。

3、优化顶层设计，注重结构保障：当务之急。

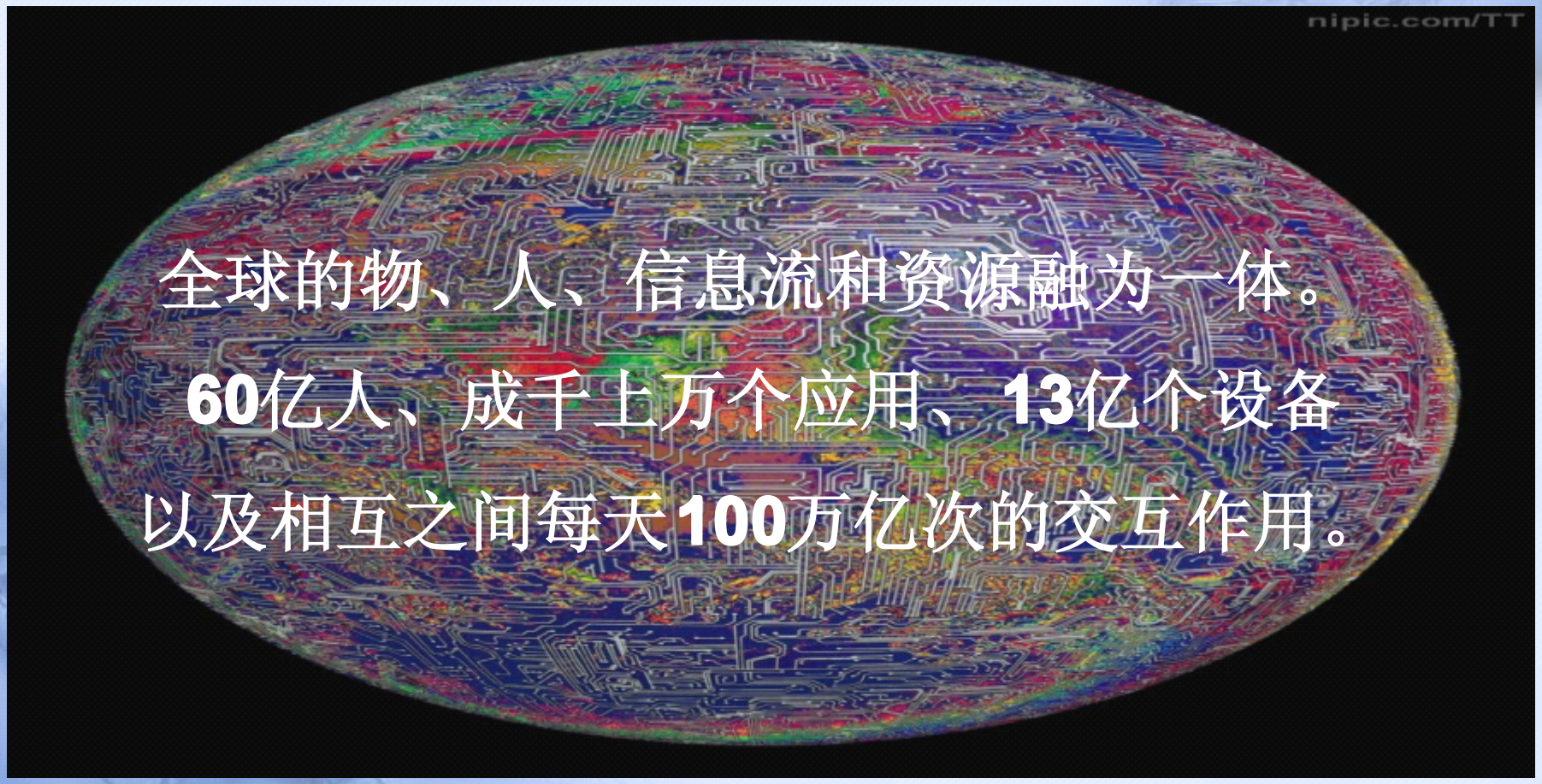
一、国外政府信息安全形势

1、信息安全环境的变化

2、美国信息安全的动向

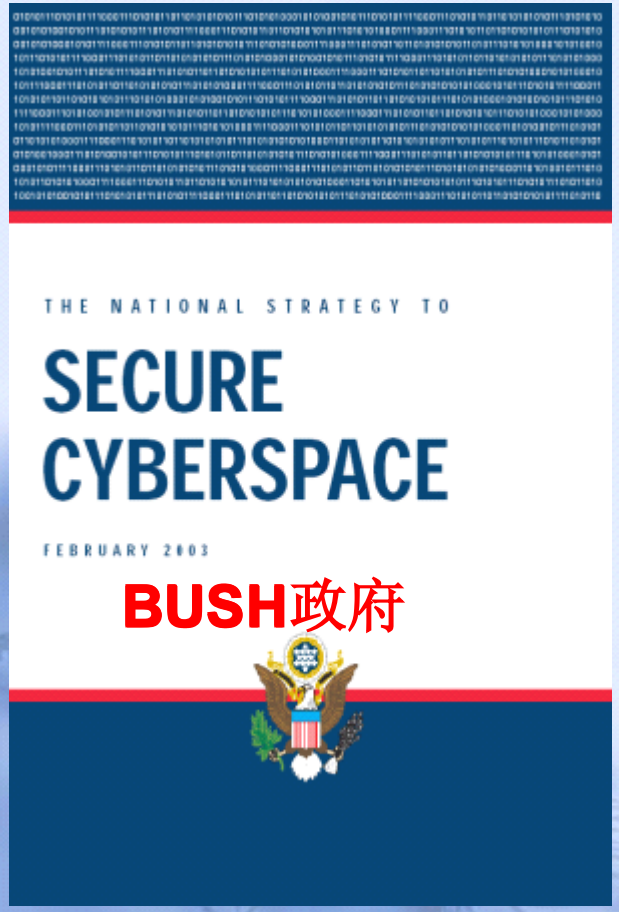
3、国际社会的战略调整

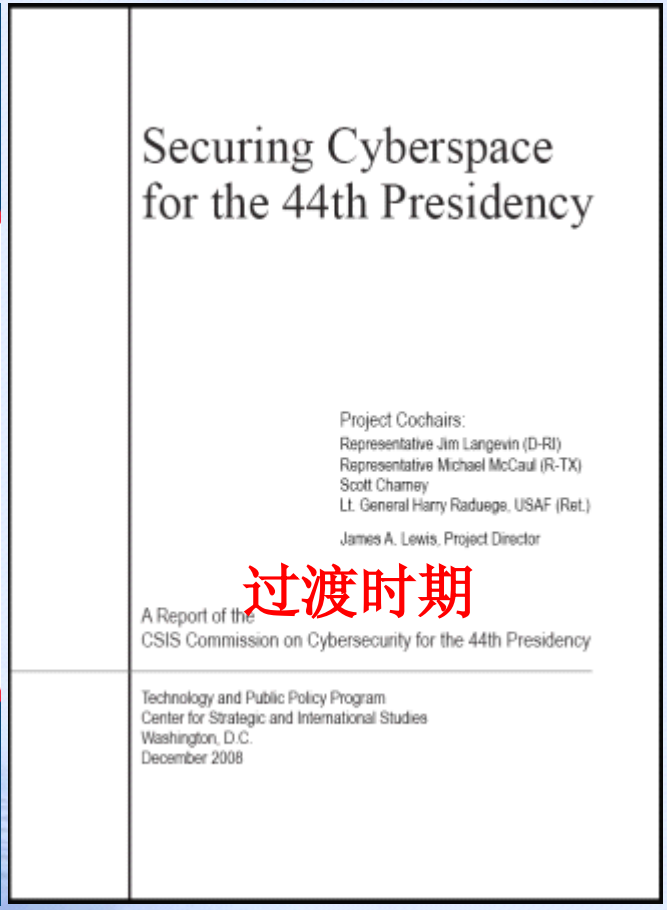
1、安全环境变化：A)全球进入物联网时期



安全环境变化：B)美国进入奥巴马时期

安全环境变化：C)信息安全进入转折时期





2、美国信息安全的动向

1、推进《国家网络空间安全战略》目标的实现；

2、实施“曼哈顿计划”（HSPD23/NSPD54总统令）；

3、优化领导体制：设立安全协调官,成立网军；

4、采取重大举措：强化信息安全保障水平；

5、加强内外合作：国内居安思危，国际合纵连横。

推进《国家网络空间安全战略》的实现

1、预防针对美国关键基础设施的网络袭击；
2、减少国家在网络安全方面的漏洞（脆弱性）；
3、降低网络攻击的损失，缩短网络恢复的时间；
4、建立国家网络安全应急响应系统；
5、制定国家网络安全威胁和漏洞减少计划；
6、确立国家网络安全意识教育和培训计划；
7、重点保护联邦政府网络的安全；
8、加强国际间的网络安全合作。

实施信息安全“曼哈顿计划”

1、可信联网--将政府机构联网点从3000多个减到100～50个以内 。

2、被动检测--部署Einstein1及Einstein2系统。

3、主动防范—开发Einstein3系统实施安全防御。

4、科研支撑—评估和研究解决信息安全新问题。

5、态势感知—设国家网络安全中心做态势监控。

6、网络反间—NSA/ FBI加强网络监控和安全调查。

7、内网安全—加强对涉密网络的安全保护。

8、教育培训—增强全民的信息安全意识和技能。

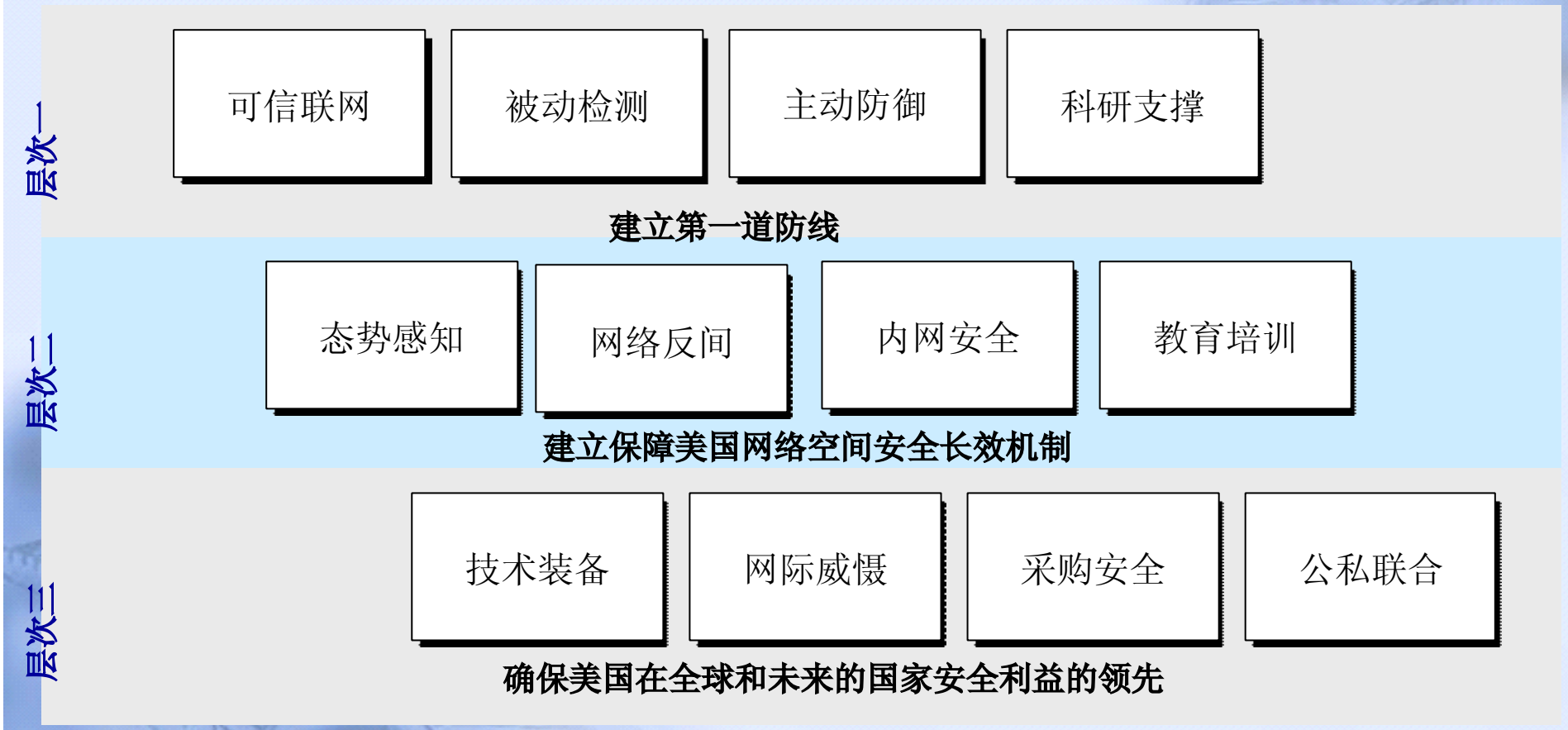
9、技术装备—研制安全防范所需的技术产品。

10、网际威慑—增强网络空间的技术和战略威慑。

11、采购安全—确保全球范围产品供应链的安全。

12、公私联合—加强政府与企业的网络安全合作。

美国政府信息安全顶层设计（CNCI）

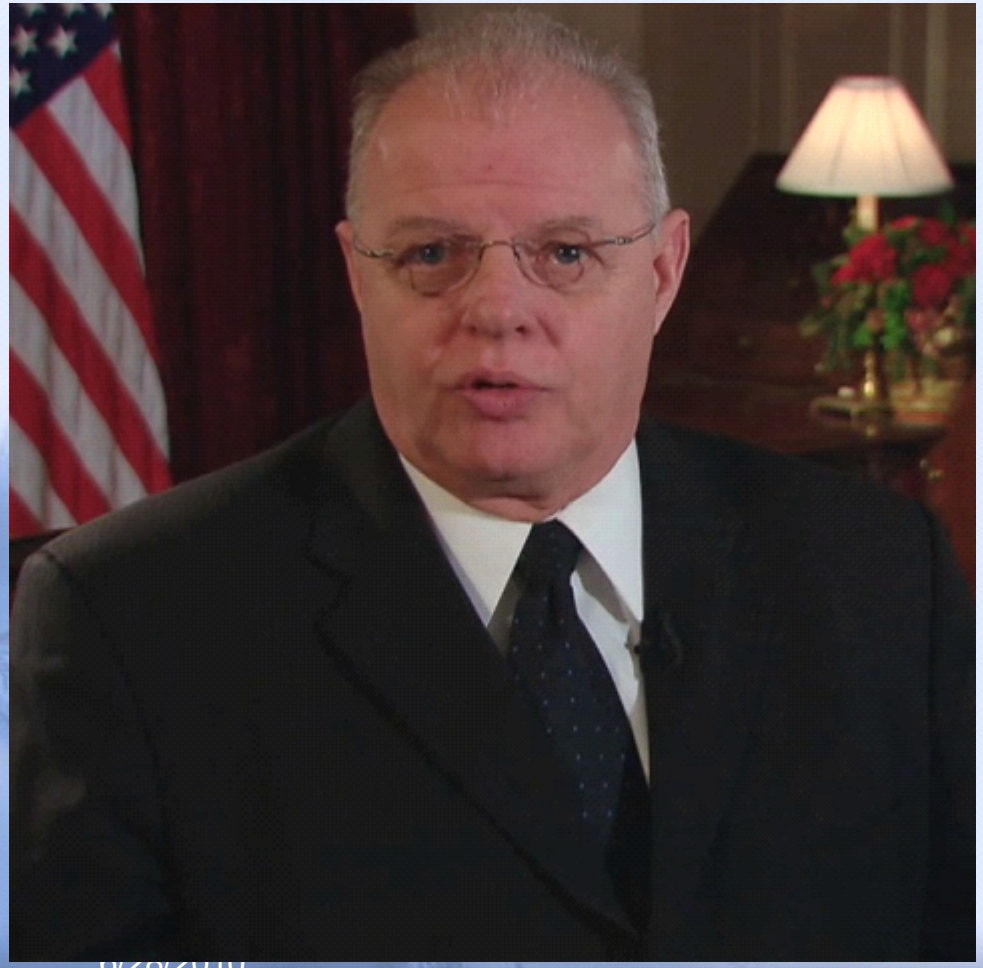


优化信息安全领导机制

- 在白宫设立网络安全办公室，任命网络安全协调官。负责统揽网络安全事务，为总统提供决策建议，协调全美网络安全力量。

- 在国防部下直接成立网络战司令部，由NSA局长担任司令；整合各军种已有的网络战力量，考虑先发制人。

网络沙皇：施密特/网军统帅：亚历山大



采取重大举措、实施重点保障

- 重点保护FEDS/CIIP:即联邦政府和电力、电信、交通、金融、应急服务、农业、食品、水、邮政、化工和公共健康等15个公共部门；
- 重点保护的方法:漏洞分析与风险管理；
- 重视科技创新，强调供应链安全。

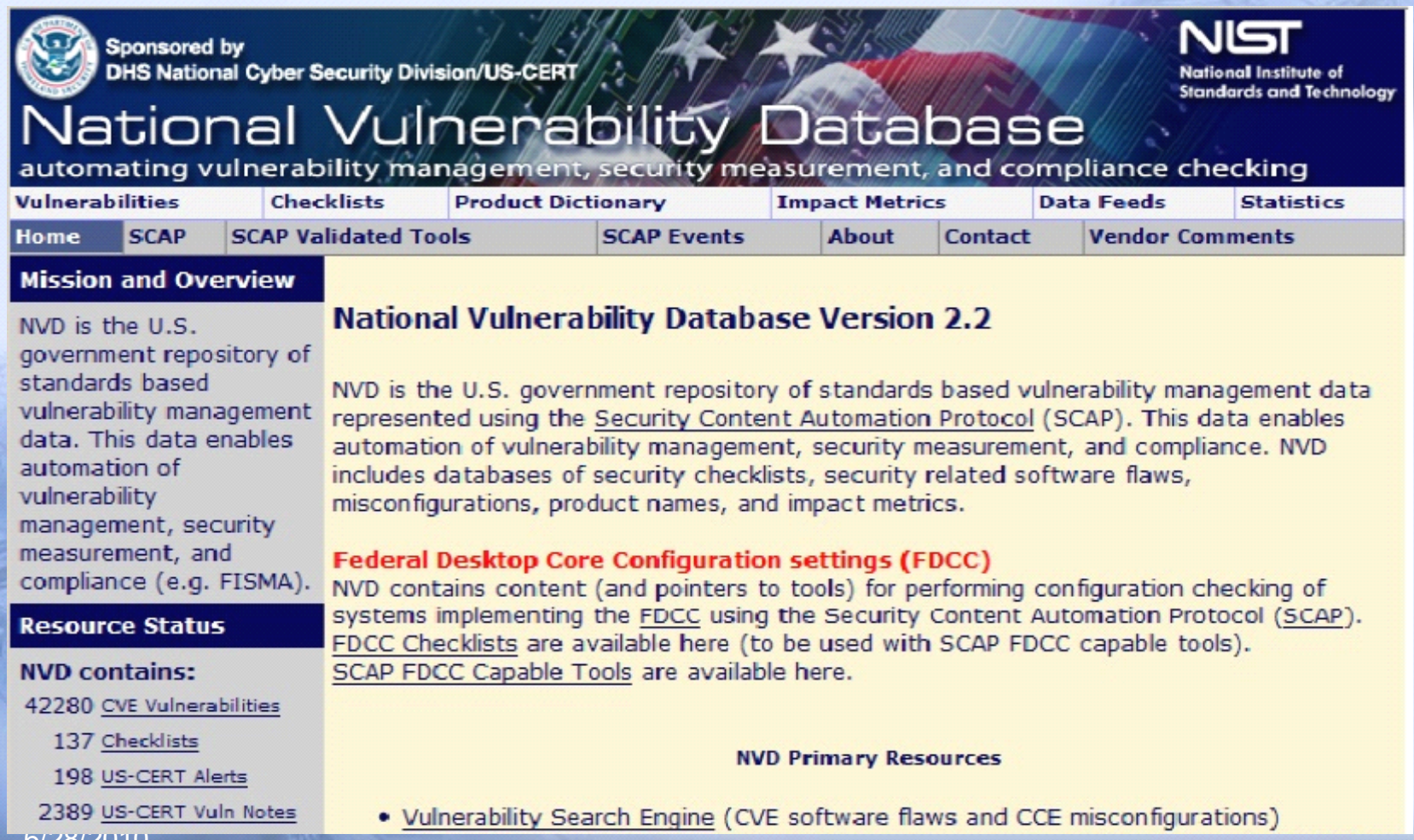
推进信息安全风险评估

在国内推进行业安全风险评估，强化对政府部门的信息安全绩效评估。

高度重视供应链的安全

利用技术优势输出霸权，严把产品进口防范隐患

美国国家漏洞库


Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
Product Dictionary
Impact Metrics
Data Feeds
Statistics
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
Mission and Overview
NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).
Resource Status
NVD contains:
42280 CVE Vulnerabilities
137 Checklists
198 US-CERT Alerts
2389 US-CERT Vuln Notes
National Vulnerability Database Version 2.2
NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.
Federal Desktop Core Configuration settings (FDCC)
NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP).
FDCC Checklists are available here (to be used with SCAP FDCC capable tools).
SCAP FDCC Capable Tools are available here.
NVD Primary Resources
• Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)

信息安全科研“跃进年”

- 启动信息安全技术研究规划，以全新的技术创意和技术路线，开展跨领域的科学研究：
  1、基于硬件的可信
  2、网络安全经济学
  3、移动目标的防御
  4、数字化DNA鉴别
  5、网络空间的健康

凝集国内民众意志

1、OBAMA总统在专题演讲中屡发居安思危之慨。

2、将加强网络安全作为《2009国家情报战略》的六大任务之一。

3、将中国视为假想敌和战略对手，大肆鼓噪“中国网络威胁论”。

4、倡导政府部门、公益机构、科研院校和公司企业等加强合作，共同应对信息安全挑战。

5、充分利用跨国公司，提高网络外交巧实力。

3、国际社会的战略调整

- 欧洲各国纷纷响应和跟进
  - 2009年6月25日，英国政府发布《网络安全空间战略》，并宣布成立网络安全办公室和网络安全运作中心
  - 2009年7月，法国成立国家网络与信息安全局，年预算9000万欧元
- 其它国家纷纷跟进
  - 澳大利亚宣布启动新的国家网络安全战略，突出重要基础设施保护
  - 韩国宣布提前于**2010**年建立网络司令部
  - 日本强调“信息安全是日本综合安保体系的核心”，加大相关设施投入。

二、我国电子政务安全环境

1、信息安全环境的变化

2、信息安全的主要隐患

3、信息安全工作的态势

1、信息安全环境的变化

安全环境A：互联网进入普及时期

- 到2009年底，基础电信企业互联网宽带接入端口已达 1.36亿个，国际出口带宽达866,367Gbps。
- 目前与国际上相互联接的海底光缆 7条，陆缆20条，总容量超过1600Gb。
- 中国境内网站达323万个，IPV4地址2.3亿多个
- 我国已建政府门户网站4.5万多个，从中央到各省、地市政府和80％以上的县级政府都建立了电子政务网站。
- 我国99.3％的乡镇和91.5％的行政村接通了互联网， 96％的乡镇接通了宽带。

安全环境B：网络成为一种社会生态

- 中国网民人数已超过3.84亿，互联网普及率达到28.9%，超过了世界平均水平。移动通信手机用户超过7亿,三网融合正快速推进。
- 80%的网站提供电子公告服务。80%以上的网民主要依靠互联网获取新闻信息。
- 66%的网民经常在网上发表言论、参与讨论和表达诉求。
- 每天通过论坛、新闻评论、博客等渠道发表的言论达300多万条。
- 2009年网民创造的网上内容达到11.4亿余篇。
- 约有2.3亿人使用搜索引擎查询信息，约2.4亿人经常用即时通信工具沟通交流，约4600万人利用互联网学习和接受教育，
- 约3500万人利用网络证券交易，约1500万人通过网络求职，约1400万人通过网络安排出行。

安全环境C：信息安全进入关键时期

- 信息技术已经渗透并影响到政治、经济、军事、文化和社会生活的各个方面；
- 我国在核心技术、高端设备和主流应用方面受制于人，技术漏洞和安全隐患日益突出；
- 信息技术安全和内容安全相互交织；
- 网络信息安全与社会稳定相互交织；
- 国内安全与国际安全问题相互交织。

2、信息安全的主要隐患

政治、社会稳定是重大威胁

网络窃密、泄密是突出威胁

技术漏洞和隐患是现实威胁

网络欺诈和犯罪是长期威胁

1）、网络群体性事件日益增多

- 2009年的77件重大公共突发事件中，有23件在网络论坛上率先暴光；
- 网上群体事件以维权居多、泄愤为主；诱发社会性骚乱的风险不断增大；
- 动员煽动面广、组织号召力强、事前预兆不多、公众参与度大、聚集速度极快等鲜明特点；
- “个案”变为“公案”、“一呼百应”发展为“一呼百万应”、“弱势群体”变为“强势团体”、“说说而已”变为“从说到做”；
- “网络曝光、舆论推动、影响扩大、问题解决 ”是网络群体事件的发酵路径。

2）、窃密、泄密，触目惊心

- 政府部门是网络窃密的重点目标，移动介质和违规联网仍是重大泄密隐患；
- 国家有关部门查处窃密案件：
  - 2007年十几起，窃取文件数量为 3万多份
  - 2008年几十起，窃取文件数量为 20多万份
  - 2009年百余起，窃取文件数量为 30多万份，
  - 已发现受控主机数量：
  - 2007年：600-1000台
  - 2008年：2000多台
  - 2009年：2000多台

3）、安全漏洞 普遍存在

- 安全漏洞在电子政务系统中普遍存在，其危害和威胁风险不断升高；
- 在被测评的数十个政务系统中，高危漏洞平均在10个以上；
- 据监测，80%的电子政务网站受到过挂马攻击；
- 在应用漏洞中，SQL注入、跨站脚本和弱口令最为突出；
- 有效执行制度化的补丁管理措施的部门不到30%，漏洞消控工作尚未进入安全保障的日程；
- 国家信息安全漏洞通报工作刚刚启动，相应的工作机制尚需完善；

4）、欺诈与犯罪 案件高发

- **2009**年我国首次成为十大网络欺诈国家之一，包括网络欺诈攻击目标和攻击发起地。
- **90%**的网民碰到过网络钓鱼（网页欺诈）。
- **21.2%**的网民表示，因为网络欺诈造成了直接的虚拟或现实财产损失。
- 木马、域名劫持，访问假网址等网络欺诈手法在面向公众的电子政务服务中呈增长趋势。

3、信息安全工作的态势

1. 重新成立国家网络与信息安全协调小组
2. 成立新一届国家信息化专家咨询委员会

3. 信息安全统一协调的职能得到加强；
4. 信息安全保密管理的工作职能加强；
5. 信息内容管理和网络治理力度加强。

信息安全保障工作重要举措

1. 多部委联合开展互联网内容综合整治行动，成效显著；
2. 党政机关反窃密、防泄密检查不断深入，收效明显；
3. 推进政府信息系统技术安全检查，提升安全保障能力；
4. 重要信息系统的风险评估工作逐步形成制度和常态；
5. 信息安全等级保护持续深入，加大督促、整改的力度；
6. 漏洞分析工作取得进展，“国家漏洞库”投入运行；
7. 进一步推进认证认可工作，产品强制认证正式启动；
8. 信息安全产业化及科研投入加大，新技术产品有突破；

三、 安全顶层设计工作建议

1、政策要求

2、安全目标

3、工作建议

电子政务信息安全政策要求

- 中办发[2002]17号文件：《关于我国电子政务建设指导意见的通知》
- 中办发[2003]27号文件：《关于加强我国信息安全保障工作的意见》
- 发改高技[2008]2071号文件：《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》
- 国办发[2009]28号文件：《政府信息系统安全检查办法》。

电子政务的安全目标

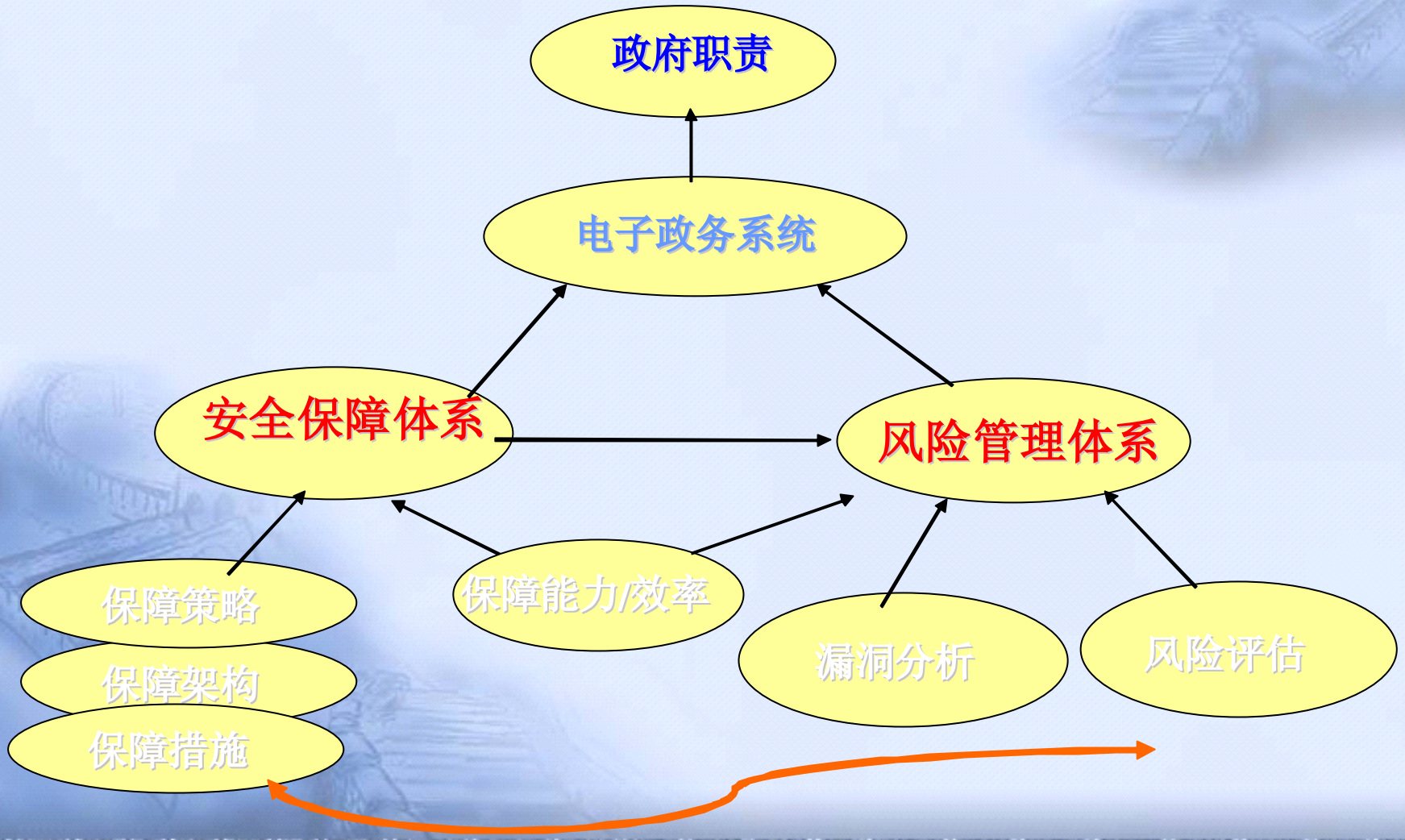
- 人员安全：可靠（防策反、防投靠）
- 信息安全：保密（防窃密、防泄密）
- 数据安全：完整（防篡改、防删除）
- 网络安全：可控（防事故、防控制）

建议1、建立一个结构化的安全体系

确保信息保密
确保网络安全
确保业务持续

可行的安全保障方案
可靠的专业技术队伍

建议2、实施两条线的安全保证



建议3、把好三个重要的管理关口

- 要严把涉密计算机和存储介质的管理关
- 要严把内部网络对外接入点线的管理关
- 要严把技术装备及服务出入网的管理关

建议4、控制四个现实的安全风险

- 门户网站：防范能力不强（软件漏洞、挂马/跳板）；
- 邮件系统：安全措施不够（弱口令、木马）；
- 保密管理：制度执行不严（U盘等移动介质、行为）；
- 服务外包：管控力度不足（供应链、运维、服务）。

建议5、落实五个长效机制的抓手

做好与信息网络相适应的安全保障体系；

做实人防与技防相结合的各项规章制度；

做到全面、及时的漏洞分析和风险评估；

做细制度化、专业化的信息安全大检查；

做勤日常信息安全保密意识教育和培训。


CHINA INFORMATION TECHNOLOGY SECURITY EVALUATION CENTER
中国信息安全测评中心
CNI SEC

敬请指正！