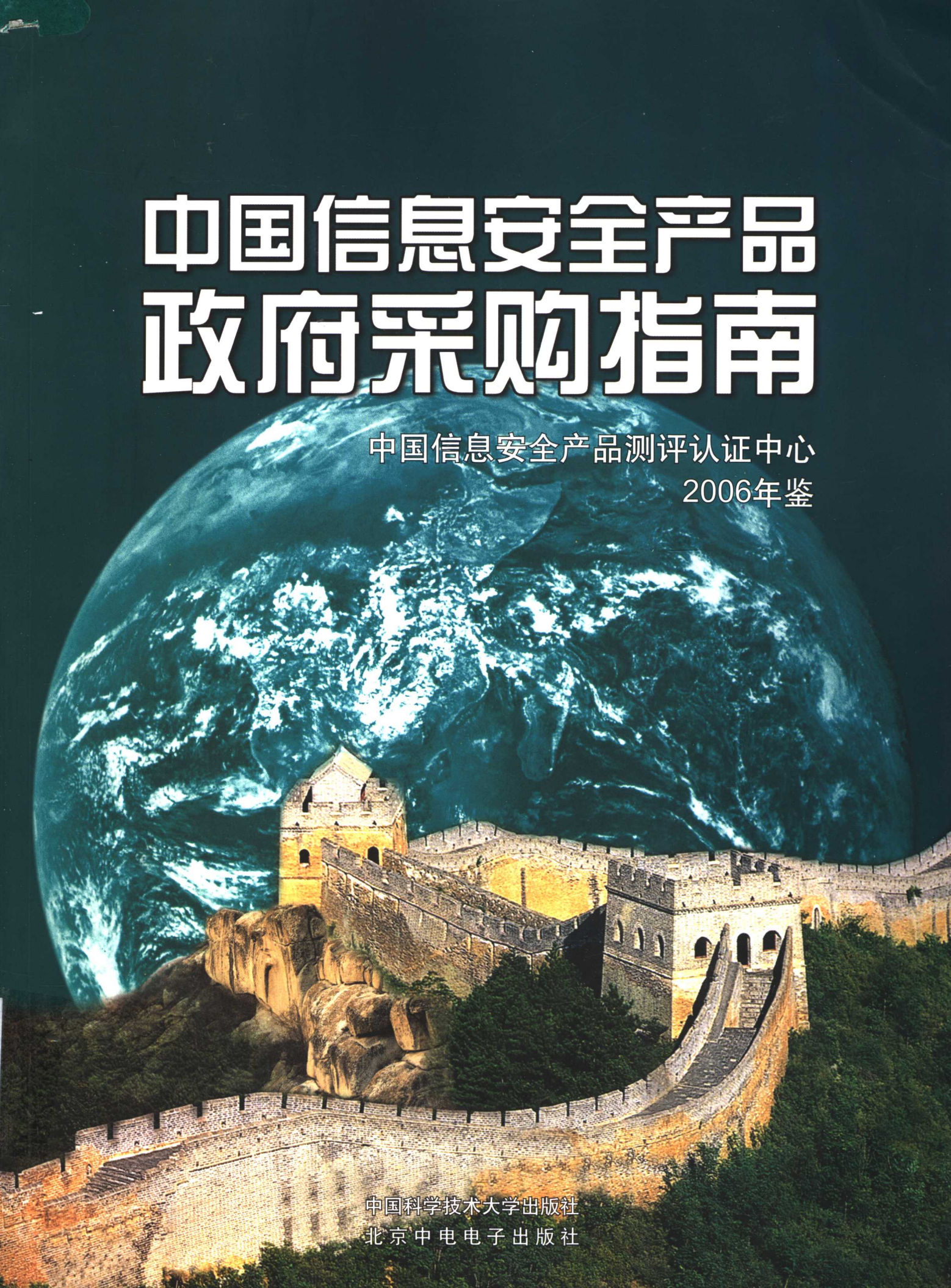
中国信息安全产品政府采购指南

中国信息安全产品测评认证中心

2006年鉴



中国科学技术大学出版社

北京中电电子出版社

中国信息安全产品

政府采购指南

2006年鉴

中国信息安全产品测评认证中心

中国科学技术大学出版社
北京中电电子出版社

内 容 简 介

本指南涵盖了2005年度获得中国信息安全产品测评认证中心测评认证的信息安全产品(八类95个)、安全服务提供商(28个)和注册信息安全专业人员(CISP)559人名单。它是继2001年度、2002年度和2004年度由中国信息安全产品测评认证中心推出的《信息安全产品政府采购指南》后的又一本新作。该书对过去一年的工作进行了回顾和总结，对热点信息安全问题予以了特别的关注和探讨。出版此书的目的是为我国政府部门采购信息安全产品、保证信息系统有效运行以及制定信息安全策略提供及时、科学、权威、公正的技术依据。

图书在版编目(CIP)数据

中国信息安全产品政府采购指南. 2006年鉴/中国信息安全产品测评认证中心编. —合肥：中国科学技术大学出版社，2006. 8

ISBN 7-312-01998-6

Ⅰ. 中… Ⅱ. 中… Ⅲ. 信息系统—安全技术—工业产品—中国—2006—手册 Ⅳ. F724.746-62

中国版本图书馆CIP数据核字(2006)第095391号

出　　版：中国科学技术大学出版社
　　(安徽省合肥市金寨路96号，230026)
　　北京中电电子出版社
　　(北京海淀区翠微东里甲2号为华大厦4层，100036)
责任编辑：邵祖英　高伟红
发　　行：中国科学技术大学出版社
印　　刷：北京华正印刷有限公司
经　　销：全国新华书店
开　　本：889×1194　1/16
印　　张：16.25
字　　数：426千字
版　　次：2006年8月第1版
印　　次：2006年8月第1次印刷
印　　数：1—3000册
定　　价：98.00元

序　言

2006 年是我国实施《2006 年 - 2020 年国家信息化发展战略》的头一年，是国务院提出的“五年时间基本建成国家信息安全保障体系目标”的第三年，也是《中华人民共和国政府采购法》施行的第四年。

我国的信息安全建设已经经历了十来个年头，十来年我国的信息安全建设经历了起步、发展和全面推进几个阶段。国家的信息安全保障工作得到逐步加强；全民的信息安全意识明显提高；国家信息安全战略已经制定；信息管理体制和工作机制逐步理顺，基础信息网络和重要信息系统的安全防护水平有所提高；互联网信息安全管理进一步加强，等级保护、风险评估工作加快推进，安全技术和产业不断发展。

十年多的信息安全实践，使我们逐步形成了几个基本概念：

(1)国家的信息安全与国家的经济安全、政治安全、文化安全合在一起是一个不可分割的整体，它们都是国家安全的有机组成部分，又都是相互作用相互关联的，四个方面的安全是从不同的侧面理解、保证国家的综合安全。因此，不能为信息安全而信息安全，而要着眼于如何保障关系国民经济命脉的关键基础设施和重要信息系统的安全，着眼于如何加快社会主义政治文明和社会主义精神文明的建设，以应对日趋激烈的国际竞争、文化渗透形势，并保持国内安全稳定的局面。

(2)信息安全又是整个国家信息化发展大局中的一个有机组成部分，不能脱离开发展的大局孤立地看待信息安全，要毫不动摇地坚持改革开放的方向，而信息安全工作中遇到的种种问题，归根到底还要靠信息化的发展来解决。

(3)发展我国信息安全事业的关键是增强安全自主创新能力，并把它作为建设创新型国家的一条重要战线。要把自主创新提高到国家战略的高度来认识，要从信息安全队伍建设和工作建设中大力弘扬创新意识、鼓励创新精神、培育创新文化。技术创新的主体是企业，要建立市场导向的产学研一体的体系，必须深化创新体制改革，并充分发挥政府的主导作用。

(4)在推动创新的诸多措施中，政府采购具有十分重要的作用，这已在很多发达国家中得到证实。政府采购作为政策工具可以优选国家自主创新的方向，可以促进自主创新转化为生产力的速度，可以降低创新产品进入市场的风险，可以保护创新企业的积极性和创造性。所以坚持出版《中国信息安全产品政府采购指南》是件很有现实意义的工作。

当前，各级政府都在积极推行电子政务，在电子政务的发展中既要增加透明度、实现信息共享，又要保护国家的机密不外泄。目前社会上安全产品质量参差不齐，为了保障政府和重点行业的信息安全，政府网络系统和重点行业必须使用经国家认证的安全产品。政府采购通过采购合格的国产信息安全产品和服务的方式支持国内企业的发展，增强我国企业的国际竞争力。

《中国信息安全产品政府采购指南》自 2002 年面世以来，受到我国政府采购部门的热烈欢迎。这本 2006 年度《中国信息安全产品政府采购指南》就是对过去工作的回顾和总结。

2005 年，中国信息安全产品测评认证中心(以下简称认证中心)在产品测评认证方面，共完成 147 项国内外产品的测评认证工作，涵盖了国内外主要信息安全产品以及重要信息技术产品。截止到 2005 年底已累计颁发 434 张产品证书，涉及厂商 150 余家，为国家信息化建设

提供了安全质量保障，为政府采购提供了权威的技术依据；在信息系统安全测评认证方面，认证中心为各政府机构、各社会用户提供了多方面、多角度、多层次的系统安全测评认证服务，为国家信息安全保障体系建设提供了有力的技术支持。据他们介绍：认证中心曾先后参与国家税务总局、国家财政部、最高人民检察院、铁道部、中国人民银行、中国证监会、国家烟草专卖局、中国联通、中国移动、中国网通以及金融、保险、石油、民航等多家党政机关、要害部门和涉及国计民生的重要网络信息系统的安全保障建设工作，在总体安全方案规划、安全咨询顾问、安全工程项目监理、信息系统安全测评认证等方面为他们提供了专业服务。尤其是在2005年，认证中心根据国务院信息化工作办公室的工作部署，圆满完成了国家税务系统风险评估试点工作；在信息安全服务资质认证方面，2005年共完成29个服务资质项目的评估工作，规范了企业服务流程，保障了服务质量。截止2005年底已向信息安全企事业单位颁发一级和二级信息安全服务资质证书87份；在信息安全人才培养方面，共颁发注册信息安全专业人员（CISP）认证证书1100多份，增强了信息安全意识，提高了信息安全人才素质。特别是2005年9月推出的注册信息安全员（CISM）资质认证，适应了我国信息化迅速发展对不同层次、不同水平和不同岗位的信息安全人才的广泛需求，进一步加大了对信息安全人才的培养范围和信息安全知识的普及和教育力度。

作为各级政府部门和信息安全厂商之间的纽带，认证中心要继续秉承并将继续坚持“科学、规范、客观、公正”的原则，严格按照国家信息安全测评认证标准及规范要求，为信息安全产品、信息系统、信息安全服务资质和信息安全人员资质的测评认证提供保障。

何德全

2006年6月

《信息安全产品政府采购指南》编委会

目 录

第 1 章　国家信息安全保障概述

1.1　温家宝主持会议通过国家信息化发展战略

国家信息化领导小组第五次会议于 2005 年 11 月 3 日在北京召开。中共中央政治局常委、国务院总理、国家信息化领导小组组长温家宝主持会议并作重要讲话。会议审议并原则通过《国家信息化发展战略（2006—2020 年）》。

温家宝指出，信息化是当今世界发展的大趋势，是推动经济社会发展和变革的重要力量。制定和实施国家信息化发展战略，是顺应世界信息化发展潮流的重要部署，是实现经济和社会发展新阶段任务的重要举措。要按照全面贯彻科学发展观的要求，站在现代化建设全局的高度，大力推进国民经济和社会信息化，不断把我国信息化提高到新水平。

中共中央政治局常委、国务院副总理、国家信息化领导小组副组长黄菊，中共中央政治局委员、国家信息化领导小组副组长周永康、郭伯雄出席会议。

会议指出，实施我国信息化发展战略，要坚持以邓小平理论和“三个代表”重要思想为指导，贯彻落实科学发展观，坚持以信息化带动工业化、以工业化促进信息化，坚持以改革开放和科技创新为动力，大力推进信息化建设，充分发挥信息化在促进经济、政治、文化、社会和军事等领域发展的重要作用，不断提高国家信息化水平，走中国特色的信息化道路，促进我国经济社会又快又好地发展。

会议强调，在制定和实施国家信息化发展战略中，要着力解决好以下问题：①坚持服务现代化建设全局，推进国民经济和社会信息化。紧紧围绕调整经济结构和转变经济增长方式，推进国民经济信息化；紧紧围绕提高治国理政能力，推行电子政务；紧紧围绕维护国家安全，推进国防和军事信息化；紧紧围绕构建和谐社会，推进社会信息化。②大力提高自主创新能力，推进创新型国家建设。努力提高原始创新、集成创新和引进消化吸收再创新能力，突破一批关键技术，掌握一批核心技术。③加快深化改革步伐，推进体制机制创新。坚持以市场和社会需求为导向，以企业为主体，充分发挥市场机制在信息化发展中的重要作用；同时加强国家宏观引导和调控，促进信息化健康发展。④夯实信息化基础，增强发展能力和服务功能。完善综合信息基础设施，开发利用全社会信息资源，提高信息产业素质和竞争力，加快制定技术标准，推进信息化法制建设。⑤注重建设信息安全保障体系，实现信息化与信息安全协调发展。⑥坚持搞好统筹协调，正确处理信息化发展中的各种重要关系。⑦加强信息化人才队伍建设，提高国民信息能力。

会议要求，各地各部门必须认真做好实施《国家信息化发展战略》的各项工作。要根据中央关于制定“十一五”规划建议和《国家信息化发展战略》的要求，抓紧制定“十一五”国家信息化发展规划。通过扎实工作，努力开创我国信息化发展的新局面。

——《国家信息安全测评认证》杂志 2005 年第 6 期

1.2 关于开展信息安全风险评估工作的意见

国家网络与信息安全协调小组（2006 年 1 月）

随着国民经济和社会信息化进程的加快，网络与信息系统的基础性、全局性作用日益增强，国民经济和社会发展对网络和信息系统的依赖性也越来越大。网络与信息系统自身存在的缺陷、脆弱性以及面临的威胁，使信息系统的运行客观上存在着潜在风险。《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发［2003］27 号）明确提出“要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理”，将开展信息安全风险评估工作作为提高我国信息安全保障水平的一项重要举措。

为推动我国信息安全风险评估工作，现提出以下意见。

1.2.1 信息安全风险评估工作的基本内容和原则

信息安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施。并为防范和化解信息安全风险，或者将风险控制在可接受的水平，从而最大限度地保障网络和信息安全提供科学依据。

信息安全风险评估分为自评估、检查评估两种形式。自评估是指网络与信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估。检查评估是指信息系统上级管理部门组织的或国家有关职能部门依法开展的风险评估。信息安全风险评估应以自评估为主，自评估和检查评估相互结合、互为补充。自评估和检查评估可依托自身技术力量进行，也可委托第三方机构提供技术支持。

信息安全风险评估工作要按照“严密组织、规范操作、讲求科学、注重实效”的原则开展。要重视和加强对信息安全风险评估工作的组织领导，完善相应的评估制度，形成预防为主、持续改进的信息安全风险评估机制。开展信息安全风险评估工作要遵循国家相关法规和信息安全管理工作的规章，参照相关标准规范及评估流程，切实把握好关键环节和评估步骤，保证信息安全风险评估工作的科学性、规范性和客观性。涉及国家秘密的信息系统的信息安全风险评估工作，必须遵循党和国家有关保密规定的要求。

1.2.2 信息安全风险评估工作的基本要求

信息安全风险评估作为信息安全保障工作的基础性工作和重要环节，应贯穿于网络和信息系统建设运行的全过程。在网络与信息系统的设计、验收及运行维护阶段均应当进行信息安全风险评估。

在网络与信息系统规划设计阶段，应通过信息安全风险评估进一步明确安全需求和安全目标；在网络与信息系统验收阶段，应通过信息安全风险评估验证已设计安装的安全措施能否实现安全目标；在网络与信息系统运行维护阶段，应定期进行信息安全风险评估工作，检验安全措施的有效性及对安全环境变化的适应性，以保障安全目标的实现。当安全形势发生重大变化或网络与信息系统使命有重大变更时，应及时进行信息安全风险评估。

要将开展信息安全风险评估作为提高信息安全管理水平的重要方法和措施。要加强网络

与信息系统规划设计阶段的信息安全风险评估，避免安全建设的盲目性。网络与信息系统的拥有、运营、使用单位要将开展信息安全风险评估工作制度化，定期组织实施网络与信息系统自评估，并积极配合有关部门的检查评估；要针对风险评估中发现的问题，提出切实有效的整改措施。有关部门要将开展信息安全风险评估作为基础信息网络和重要信息系统规划、建设和落实等级保护工作要求的重要内容，并对有关经费予以保障。

信息安全风险评估工作敏感性强，涉及网络与信息系统的关键资产和核心信息，网络与信息系统的拥有、运营、使用单位和主管部门要按照“谁主管谁负责，谁运营谁负责”的原则，切实负起严格管理的责任。参与信息安全风险评估工作的单位及其有关人员均应遵守国家有关信息安全和保密的法律法规，并承担相应的责任和义务。信息安全风险评估工作可能涉及个人隐私、工作或商业敏感信息，甚至国家秘密信息，风险评估工作的发起方必须与参与评估的有关单位或人员签订具有法律约束力的保密协议。

国家基础信息网络和关系国计民生的重要信息系统的信息安全风险评估工作，应按有关规定进行。

1.2.3　开展信息安全风险评估工作的有关安排

加强信息安全风险评估的基础性工作。要加快制定和完善信息安全风险评估有关技术标准，尽快完善并颁布《信息安全风险评估指南》和《信息安全风险管理指南》等国家标准。各行业主管部门也可根据本行业特点制定相应的技术规范。重视信息安全风险评估核心技术、方法和工具的研究与攻关，积极开展信息安全风险评估的培训与交流。抓紧研究制定有关信息安全服务资质的管理办法。加强信息安全风险意识的宣传教育，加快培养信息安全风险评估的专门人才。

加强信息安全风险评估工作的组织领导。各信息化和信息安全主管部门要充分认识风险评估工作对于提高信息安全管理水平的重要意义，高度重视对风险评估工作的组织领导，切实加强对风险评估工作的管理，抓紧制定贯彻落实的办法，积极稳妥地推进。要从抓试点开始，逐步探索组织实施和管理的经验，用三年左右的时间在我国基础信息网络和重要信息系统普遍推行信息安全风险评估工作，全面提高我国信息安全的科学管理水平，提升网络与信息系统安全保障能力，为保障和促进我国信息化发展服务。

——《国家信息安全测评认证》杂志 2006 年第 2 期

1.3　信息安全保障工作重在落实

国务院信息化工作办公室网络与安全组　王渝次司长

2004 年是我国信息安全保障工作至关重要的一年。年初召开了全国信息安全保障工作会议，中央政治局常委、国务院副总理黄菊出席会议并作了重要讲话。会议在《国家信息化领导关于加强信息安全保障工作的意见》（中办发［2003］27 号文）基础上，进一步明确了我国信息安全保障工作的指导方针、基本原则和主要任务，确立了用五年左右的时间基本建成国家信息安全保障体系的工作目标。党的十六届四中全会，更是把信息安全和政治安全、经济安全、文化安全放在同等重要的位置，这在我们党的历史上是前所未有的。所有这些，都标志着我国的信息安全保障工作进入了一个崭新的阶段。

经过一年的努力，我国信息安全保障工作取得了明显的成效：随着27号文件的颁布和国家信息安全战略研究、《信息安全条例》起草工作的积极推进，信息安全的顶层设计基本上完整了，信息安全整体框架清晰了；信息安全管理体制和工作机制逐步建立，信息安全责任制基本落实；信息安全等级保护、信息安全风险评估、信息安全产品认证认可、信息安全应急协调机制建设、网络信任体系建设、信息安全标准化制定等基础性工作和基础设施建设取得较大进展；信息安全问题受到了全社会前所未有的普遍关注，人们对信息安全的理解和认识更加深入全面。信息安全保障工作的局面已经打开，这种崭新的局面为进一步维护国家信息安全、保障信息化健康发展打下了良好的基础。

建设国家信息安全保障体系，是一项复杂的、综合的系统工程，是坚持积极防御、综合防范方针的具体体现。这是我国信息化建设和信息安全保障的客观要求，是信息安全保障规律与特点的客观体现，也是各国信息安全保障普遍经验的客观总结。坚持积极防御、综合防范方针，就是要充分认识信息化建设中的安全风险与威胁，综合平衡信息安全风险与成本，做到信息化建设与信息安全保障同步规划、同步建设、同步使用；就是要用发展的思路解决信息安全问题，强调以安全保发展、在发展中求安全，不是被动地就安全抓安全；就是要综合运用行政、法律、技术、管理等多种手段，充分发挥各方面的积极性，各部门齐抓共管、全社会共同参与，用系统工程的思路，用体系建设的思路来保障信息安全。

当前和今后一段时间，是我国国民经济和社会信息化快速发展期，如果信息安全保障工作跟不上，就会拖信息化发展的后腿，拖国家发展的后腿。因此，加强信息安全保障工作，建设国家信息安全保障体系，是大势所趋，是时代要求，不仅要建，而且要争取早日建成。按时间算，用五年时间基本建成信息安全保障体系，任务紧迫，时不我待。而我们还有很多事情没有做，或者还没有落到实处。而且这样一个庞大的系统工程的确不是一蹴而就的，需要我们费很大的气力来抓，需要各个方面共同努力、紧抓不懈。

为此，2005年我们的工作任务仍然是继续坚定不移地贯彻落实27号文件和全国信息安全保障工作会议提出的各项任务，扎扎实实地抓好基础性工作和基础设施建设，继续推进信息安全等级保护、信息安全风险评估、信息安全产品认证认可等基础性工作；继续加快以密码技术为基础的信息保护和网络信任体系建设，进一步完善应急协调机制与灾难备份工作；按照中央要求，进一步加强互联网管理，创建安全、健康、有序的网络环境；进一步创建产业发展环境支持信息安全产业发展，加快信息安全学科建设和人才培养，加强国际合作与交流，完善信息安全的管理体制和机制。2005年是“十五”的最后一年，国家有关部门正在按照中央的要求抓紧制定国家“十一五”信息安全专项规划、“十一五”信息安全科技发展规划和“十一五”信息安全产业发展规划，这将大大推进国家信息安全保障体系的建设。可以预期，经过全社会的共同努力，我们终将克服前进过程中的各种困难，早日建成国家信息安全保障体系，努力完成国家和时代赋予我们的神圣使命。

信息安全保障工作正处于一个非常好的历史发展时期。国家为信息安全的发展创造了良好的政策环境，这是我们发展信息安全的极为有利的条件。众所周知，信息安全是一个技术性非常强的高技术对抗领域。我们要确保我国的信息安全，必须不断加大技术研发和自主创新的力度，特别是应当着力于关键领域的技术攻关，加强信息安全技术平台的建设。在这方面，我们的企业应当多一些战略的眼光，从长远出发，发展壮大自己。

应该看到，我们的国内企业在信息安全产业发展、特别是在安全服务方面具有独特的优势。尤其要指出的是，我们一定要高度重视信息安全服务产业的发展。国家已经提出建立健全信息安全市场服务体系，包括面向社会的技术咨询与培训，提供风险评估服务，承担信息

安全工程，政府信息系统的托管，建立数据仓库为社会服务，建立基础设施为信息化建设提供支撑等等。国内企业占有天时地利人和的优势，我希望我们的企业一定要紧紧抓住机遇，靠技术实力、管理实力，靠拼搏精神，靠服务质量和服务水平，做实、做大、做强。我相信，在不远的将来，我们国家会出现一些颇具份量的信息安全优秀品牌，会带动整个信息安全产业的发展。

——王渝次司长在“第五届中国信息安全发展趋势与战略”高层研讨会上的讲话

1.4　发展核心技术　建立自主完整的软件产业体系

中国工程院院士　倪光南

1.4.1　没有核心技术就没有信息安全

信息领域的核心技术在很大程度上影响着信息安全。例如计算机的CPU和操作系统这些核心技术如果不是自主开发的（或完全开放的）产品，使用这样的计算机就会存在很大的安全隐患。由于这些核心技术非常复杂，如果使用别人的产品，几乎不可能验证其安全性，不可能达到自主、可控。因此，无论是从国家的信息安全保障还是从长远发展来说，一定要发展自己的IT核心技术。只有这样，才能提高企业的竞争力，取得高利润，确保信息安全；也只有这样，才能掌握产业发展的主动权、实现持续的发展。

过去，我们没有掌握这些核心技术，近年来国家大力倡导自主创新，中国逐渐发展出自主的核心技术，开放源代码软件也促进了自主核心技术的发展。中国现在已有许多单位研制出了CPU，操作系统等基础软件也从无到有逐渐发展起来。例如，在历来被Windows垄断的操作系统领域，许多公司推出了适合中国用户使用的Linux操作系统（有红旗、中标普华、新华等版本），它们在电子政务等有关国计民生的信息系统中可以取代Windows，更好地保障信息安全，节约信息化开支；龙芯、C＊Core、众志、THUMP等国产CPU纷纷推出，采用国产CPU的网络计算机在窗口服务型行业和内部办公系统等处逐步取代某些PC。永中、WPS、Red Office等国产办公套件也已可基本替代微软Office，满足电子政务等应用需求。上述事实表明：在创新思维的指导下，近年来我国自主的核心技术获得可喜的进展。

1.4.2　我国当前信息技术大环境和主要存在的问题

虽然这些年中国的核心技术研发取得了令人欣慰的成就，但是从当前整个信息技术的大环境和发展现状来看，并不容太多的乐观。

中国从消费层面看是信息产业大国，但技术上却不是信息产业强国，其最突出的表现便是在集成电路与软件两方面。在计算机产业中，核心的芯片技术，操作系统都由英特尔、微软把持，尽管我国年产PC超过1000万台，但中国企业大多从事技术含量低、利润微薄的加工、装配，处于受别人控制和影响的下游。中国的许多企业处于“大进大出”，尽管产能高，但要向上游的芯片厂商、操作系统厂商交大笔采购费和权利金，好看的数字下面掩盖着亏损的危机。近年来，中国在CPU等芯片方面，在Linux等基础软件方面，取得了相当的成就，但这些技术产业化推动力量不够，所占市场份额不够。

因此，我们一定要清醒地认识到这一点，目前来说，我们可以称得上是信息产业大国，但却不是信息产业强国，而要改变这一现状的最根本的途径就是要大力发展具有自主知识产