关于印送《关于开展信息安全等级保护

安全建设整改工作的指导意见》的函

公信安[2009]1429号

中央和国家机关各部委，国务院各直属机构、办事机构、事业单位：

为进一步贯彻落实国家信息安全等级保护制度，指导各地区、各部门在信息安全等级保护定级工作基础上，深入开展信息安全等级保护安全建设整改工作，我部制定了《关于开展信息安全等级保护安全建设整改工作的指导意见》。现印送给你们，请在实际工作中参照。

            二〇〇九年十月二十七日

抄送：中央企业。

各省、自治区、直辖市信息安全等级保护工作协调（领导）小组。

关于开展信息安全等级保护

安全建设整改工作的指导意见

为进一步贯彻落实《国家信息化领导小组关于加强信息安全保障工作的意见》和《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》（以下简称《管理办法》）精神，指导各部门在信息安全等级保护定级工作基础上，开展已定级信息系统（不包括涉及国家秘密信息系统）安全建设整改工作，特提出如下意见：

一、明确工作目标

依据信息安全等级保护有关政策和标准，通过组织开展信息安全等级保护安全管理制度建设、技术措施建设和等级测评，落实等级保护制度的各项要求，使信息系统安全管理水平明显提高，安全防范能力明显增强，安全隐患和安全事故明显减少，有效保障信息化健康发展，维护国家安全、社会秩序和公共利益，力争在2012年底前完成已定级信息系统安全建设整改工作。

二、细化工作内容

（一）开展信息安全等级保护安全管理制度建设，提高信息系统安全管理水平。按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，建立健全并落实符合相应等级要求的安全管理制度：一是信息安全责任制，明确信息安全工作的主管领导、责任部门、人员及有关岗位的信息安全责任；二是人员安全管理制度，明确人员录用、离岗、考核、教育培训等管理内容；三是系统建设管理制度，明确系统定级备案、方案设计、产品采购使用、密码使用、软件开发、工程实施、验收交付、等级测评、安全服务等管理内容；四是系统运维管理制度，明确机房环境安全、存储介质安全、设备设施安全、安全监控、网络安全、系统安全、恶意代码防范、密码保护、备份与恢复、事件处置、应急预案等管理内容。建立并落实监督检查机制，定期对各项制度的落实情况进行自查和监督检查。

（二）开展信息安全等级保护安全技术措施建设，提高信息系统安全保护能力。按照《管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全等级保护实施指南》、《信息系统通用安全技术要求》、《信息系统安全工程管理要求》、《信息系统等级保护安全设计技术要求》等标准规范要求，结合行业特点和安全需求，制定符合相应等级要求的信息系统安全技术建设整改方案，开展信息安全等级保护安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，建立并完善信息系统综合防护体系，提高信息系统的安全防护能力和水平。

（三）开展信息系统安全等级测评，使信息系统安全保护状况逐步达到等级保护要求。选择由省级（含）以上信息安全等级保护工作协调小组办公室审核并备案的测评机构，对第三级（含）以上信息系统开展等级测评工作。等级测评机构依据《信息系统安全等级保护测评要求》等标准对信息系统进行测评，对照相应等级安全保护要求进行差距分析，排查系统安全漏洞和隐患并分析其风险，提出改进建议，按照公安部制订的信息系统安全等级测评报告格式编制等级测评报告。经测评未达到安全保护要求的，要根据测评报告中的改进建议，制定整改方案并进一步进行整改。各部门要及时向受理备案的公安机关提交等级测评报告。对于重要部门的第二级信息系统，可以参照上述要求开展等级测评工作。

三、落实工作要求

（一）统一组织，加强领导。要按照“谁主管、谁负责”的原则，切实加强对信息安全等级保护安全建设整改工作的组织领导，完善工作机制。要结合各自实际，统一规划和部署安全建设整改工作，制定安全建设整改工作实施方案。要落实责任部门、责任人员和安全建设整改经费。要利用多种形式，组织开展宣传、培训工作。

（二）循序渐进，分步实施。信息系统主管部门可以结合本行业、本部门信息系统数量、等级、规模等实际情况，按照自上而下或先重点后一般的顺序开展。重点行业、部门可以根据需要和实际情况，选择有代表性的第二、三、四级信息系统先进行安全建设整改和等级测评工作试点、示范，在总结经验的基础上全面推开。

（三）结合实际，制定规范。重点行业信息系统主管部门可以按照《信息系统安全等级保护基本要求》等国家标准，结合行业特点，确定《信息系统安全等级保护基本要求》的具体指标；在不低于等级保护基本要求的情况下，结合系统安全保护的特殊需求，在有关部门指导下制定行业标准规范或细则，指导本行业信息系统安全建设整改工作。

（四）认真总结，按时报送。自2009年起，要对定级备案、等级测评、安全建设整改和自查等工作开展情况进行年度总结，于每年年底前报同级公安机关网安部门，各省（自治区、直辖市）公安机关网安部门报公安部网络安全保卫局。信息系统备案单位每半年要填写《信息安全等级保护安全建设整改工作情况统计表》并报受理备案的公安机关。