公　　安　　部
国　家　保　密　局
国 家 密 码 管 理　局
国务院信息化工作办公室
文件

公通字[2004]66 号

关于印发《关于信息安全等级保护工作的实施意见》的通知

各省、自治区、直辖市公安厅（局）、保密局、国家密码管理委员会办公室、信息化领导小组办公室，新疆生产建设兵团公安局、保密局、国家密码管理委员会办公室、信息化领导小组办公室，中央和国家机关各部委保密委员会办公室，各人民团体保密委员会办公室：

《关于信息安全等级保护工作的实施意见》已经国家网络与信

息安全协调小组第三次会议讨论通过，现印发给你们，请认真贯彻实施。

公安部　　国家保密局

国家密码管理委员会办公室　　国务院信息化工作办公室

二00四年九月十五日

主题词：信息 安全　等级 保护　实施 意见

抄送：中央办公厅，国务院办公厅。中央政法委、中央610办公室，发展改革委、教育部、科技部、安全部、财政部、信息产业部、铁道部、中国人民银行、海关总署、税务总局、民航总局、广电总局、国务院新闻办、中国证券监督管理委员会，国家电网公司。

公安部办公厅　　2004年9月17日印发

承办人：郭启全　　校对：张俊兵

关于信息安全等级保护工作的实施意见

信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。实行信息安全等级保护制度，能够充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到有效保护的目的，增强安全保护的整体性、针对性和实效性，使信息系统安全建设更加突出重点、统一规范、科学合理，对促进我国信息安全的发展将起到重要推动作用。

为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。2003年中央办公厅、国务院办公厅转发的《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）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

一、开展信息安全等级保护工作的重要意义

近年来，党中央、国务院高度重视，各有关方面协调配合、共同努力，我国信息安全保障工作取得了很大进展。但是从总体上看，

我国的信息安全保障工作尚处于起步阶段，基础薄弱，水平不高，存在以下突出问题：信息安全意识和安全防范能力薄弱，信息安全滞后于信息化发展；信息系统安全建设和管理的目标不明确；信息安全保障工作的重点不突出；信息安全监督管理缺乏依据和标准，监管措施有待到位，监管体系尚待完善。随着信息技术的高速发展和网络应用的迅速普及，我国国民经济和社会信息化进程全面加快，信息系统的基础性、全局性作用日益增强，信息资源已经成为国家经济建设和社会发展的重要战略资源之一。保障信息安全，维护国家安全、公共利益和社会稳定，是当前信息化发展中迫切需要解决的重大问题。

实施信息安全等级保护，能够有效地提高我国信息和信息系统安全建设的整体水平，有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调；有利于为信息系统安全建设和管理提供系统性、针对性、可行性的指导和服务，有效控制信息安全建设成本；有利于优化信息安全资源的配置，对信息系统分级实施保护，重点保障基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统的安全；有利于明确国家、法人和其他组织、公民的信息安全责任，加强信息安全管理；有利于推动信息安全产业的发展，逐步探索出一条适应社会主义市场经济发展的信息安全模式。

二、信息安全等级保护制度的原则

信息安全等级保护的核心是对信息安全分等级、按标准进行建设、管理和监督。信息安全等级保护制度遵循以下基本原则：

（一）明确责任，共同保护。通过等级保护，组织和动

员国家、法人和其他组织、公民共同参与信息安全保护工作；各方主体按照规范和标准分别承担相应的、明确具体的信息安全保护责任。

（二）依照标准，自行保护。国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定级、自行保护。

（三）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

（四）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统，主要包括：国家事务处理信息系统（党政机关办公系统）；财政、金融、税务、海关、审计、工商、社会保障、能源、交通运输、国防工业等关系到国计民生的信息系统；教育、国家科研等单位的信息系统；公用通信、广播电视传输等基础信息网络中的信息系统；网络管理中心、重要网站中的重要信息系统和其他领域的重要信息系统。

三、信息安全等级保护制度的基本内容

信息安全等级保护是指对国家秘密信息、法人和其他组织及公

民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

信息系统是指由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。

根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；针对信息的保密性、完整性和可用性要求及信息系统必须要达到的基本的安全保护水平等因素，信息和信息系统的安全保护等级共分五级：

1. 第一级为自主保护级，适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益。

2. 第二级为指导保护级，适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害。

3. 第三级为监督保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害。

4. 第四级为强制保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害。

5. 第五级为专控保护级，适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。

国家通过制定统一的管理规范和技术标准，组织行政机关、公民、法人和其他组织根据信息和信息系统的不同重要程度开展有针对性的保护工作。国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策。第一级依照国家管理规范和技术标准进行自主保护；第二级在信息安全监管职能部门指导下依照国家管理规范和技术标准进行自主保护；第三级依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行监督、检查；第四级依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查；第五级依照国家管理规范和技术标准进行自主保护，国家指定专门部门、专门机构进行专门监督。

国家对信息安全产品的使用实行分等级管理。

信息安全事件实行分等级响应、处置的制度。依据信息安全事件对信息和信息系统的破坏程度、所造成的社会影响以及涉及的范围，确定事件等级。根据不同安全保护等级的信息系统中发生的不同等级事件制定相应的预案，确定事件响应和处置的范围、程度以及适用的管理制度等。信息安全事件发生后，分等级按照预案响应和处置。

四、信息安全等级保护工作职责分工

公安机关负责信息安全等级保护工作的监督、检查、指导。国家保密工作部门负责等级保护工作中有关保密工作的监督、检查、

指导。国家密码管理部门负责等级保护工作中有关密码工作的监督、检查、指导。

在信息安全等级保护工作中，涉及其他职能部门管辖范围的事项，由有关职能部门依照国家法律法规的规定进行管理。

信息和信息系统的主管部门及运营、使用单位按照等级保护的管理规范和技术标准进行信息安全建设和管理。

国务院信息化工作办公室负责信息安全等级保护工作中部门间的协调。

五、实施信息安全等级保护工作的要求

信息安全等级保护工作要突出重点、分级负责、分类指导、分步实施，按照谁主管谁负责、谁运营谁负责的要求，明确主管部门以及信息系统建设、运行、维护、使用单位和个人的安全责任，分别落实等级保护措施。实施信息安全等级保护应当做好以下六个方面工作：

（一）完善标准，分类指导。制定系统完整的信息安全等级保护管理规范和技术标准，并根据工作开展的实际情况不断补充完善。信息安全监管职能部门对不同重要程度的信息和信息系统的安全等级保护工作给予相应的指导，确保等级保护工作顺利开展。

（二）科学定级，严格备案。信息和信息系统的运营、使用单位按照等级保护的管理规范和技术标准，确定其信息和信息系统的安全保护等级，并报其主管部门审批同意。

对于包含多个子系统的信息系统，在保障信息系统安全互联和有效信息共享的前提下，应当根据等级保护的管理规定、技术标准

和信息系统内各子系统的重要程度，分别确定安全保护等级。跨地域的大系统实行纵向保护和属地保护相结合的方式。

国务院信息化工作办公室组织国内有关信息安全专家成立信息安全保护等级专家评审委员会。重要的信息和信息系统的运营、使用单位及其主管部门在确定信息和信息系统的安全保护等级时，应请信息安全保护等级专家评审委员会给予咨询评审。

安全保护等级在三级以上的信息系统，由运营、使用单位报送本地区地市级公安机关备案。跨地域的信息系统由其主管部门向其所在地的同级公安机关进行总备案，分系统分别由当地运营、使用单位向本地地市级公安机关备案。

信息安全产品使用的分等级管理以及信息安全事件分等级响应、处置的管理办法由公安部会同保密局、国密办、信息产业部和认监委等部门制定。

（三）建设整改，落实措施。对已有的信息系统，其运营、使用单位根据已经确定的信息安全保护等级，按照等级保护的管理规范和技术标准，采购和使用相应等级的信息安全产品，建设安全设施，落实安全技术措施，完成系统整改。对新建、改建、扩建的信息系统应当按照等级保护的管理规范和技术标准进行信息系统的规划设计、建设施工。

（四）自查自纠，落实要求。信息和信息系统的运营、使用单位及其主管部门按照等级保护的管理规范和技术标准，对已经完成安全等级保护建设的信息系统进行检查评估，发现问题及时整改，加强和完善自身信息安全等级保护制度的建设，加强自我保护。

（五）建立制度，加强管理。信息和信息系统的运营、使用单位按照与本系统安全保护等级相对应的管理规范和技术标准的要求，定期进行安全状况检测评估，及时消除安全隐患和漏洞，建立安全制度，制定不同等级信息安全事件的响应、处置预案，加强信息系统的安全管理。信息和信息系统的主管部门应当按照等级保护的管理规范和技术标准的要求做好监督管理工作，发现问题，及时督促整改。

（六）监督检查，完善保护。公安机关按照等级保护的管理规范和技术标准的要求，重点对第三、第四级信息和信息系统的安全等级保护状况进行监督检查。发现确定的安全保护等级不符合等级保护的管理规范和技术标准的，要通知信息和信息系统的主管部门及运营、使用单位进行整改；发现存在安全隐患或未达到等级保护的管理规范和技术标准要求的，要限期整改，使信息和信息系统的安全保护措施更加完善。对信息系统中使用的信息安全产品的等级进行监督检查。

对第五级信息和信息系统的监督检查，由国家指定的专门部门、专门机构按照有关规定进行。

国家保密工作部门、密码管理部门以及其他职能部门按照职责分工指导、监督、检查。

六、信息安全等级保护工作实施计划

计划用三年左右的时间在全国范围内分三个阶段实施信息安全等级保护制度。

（一）准备阶段。为了保障信息安全等级保护制度的顺利

实施，在全面实施等级保护制度之前，用一年左右的时间做好下列准备工作：

1.加强领导，落实责任。在国家网络与信息安全协调小组的领导下，地方各级人民政府、信息安全监管职能部门、信息系统的主管部门和运营、使用单位要明确各自的安全责任，建立协调配合机制，分别制定详细的实施方案，积极推进信息安全等级保护制度的建立，推动信息安全管理运行机制的建立和完善。

2.加快完善法律法规和标准体系。法律规范和技术标准是推广和实施信息安全等级保护工作的法律依据和技术保障。为此，《信息安全等级保护管理办法》和《信息安全等级保护实施指南》、《信息安全等级保护评估指南》等法规、规范要加紧制定，尽快出台。

加快信息安全等级保护管理与技术标准的制定和完善，其他现行的相关标准规范中与等级保护管理规范和技术标准不相适应的，应当进行调整。

3.建设信息安全等级保护监督管理队伍和技术支撑体系。信息安全监管职能部门要建立专门的信息安全等级保护监督检查机构，充实力量，加强建设，抓紧培训，使监督检查人员能够全面掌握信息安全等级保护相关法律规范和管理规范及技术标准，熟练运用技术工具，切实承担信息安全等级保护的指导、监督、检查职责。同时，还要建立信息安全等级保护监督、检查工作的技术支撑体系，组织研制、开发科学、实用的检查、评估工具。

4.进一步做好等级保护试点工作。选择电子政务、电子商务以及其他方面的重点单位开展等级保护试点工作，并在试点工作的基础上进一步完善等级保护实施指南等相关的配套规范、标准和工

具，积累信息安全等级保护工作实施的方法和经验。

5.加强宣传、培训工作。地方各级人民政府、信息安全监管职能部门和信息系统的主管部门要积极宣传信息安全等级保护的相关法规、标准和政策，组织开展相关培训，提高对信息安全等级保护工作的认识和重视，积极推动各有关部门、单位做好开展信息安全等级保护工作的前期准备。

（二）重点实行阶段。在做好前期准备工作的基础上，用一年左右的时间，在国家重点保护的涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统中实行等级保护制度。经过一年的建设，使基础信息网络和重要信息系统的核心要害部位得到有效保护，涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统的保护状况得到较大改善，结束目前基本没有保护措施或保护措施不到位的状况。

在工作中，如发现等级保护的管理规范和技术标准以及检查评估工具等存在问题，及时组织有关部门进行调整和修订。

（三）全面实行阶段。在试行工作的基础上，用一年左右的时间，在全国全面推行信息安全等级保护制度。已经实施等级保护制度的信息和信息系统的运营、使用单位及其主管部门，要进一步完善信息安全保护措施。没有实施等级保护制度的，要按照等级保护的管理规范和技术标准认真组织落实。

经过三年的努力，逐步将信息安全等级保护制度落实到信息安全规划、建设、评估、运行维护等各个环节，使我国信息安全保障状况得到基本改善。