 关于开展保险业信息系统安全等级保护定级工作的通知 保监厅发〔2007〕45号各保监局，各保险公司、保险资产治理公司，中国保险行业协会： 为贯彻落实国家信息安全等级保护制度，按照《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861号）要求，中国保监会将在保险行业内开展信息系统安全等级保护定级工作。现将有关事项通知如下： 一、等级保护定级工作的要求及组织方式 各单位应按照“ 准确定级、严格审批、及时备案、认真整改、科学测评 ”的要求和“ 自主定级、自主保护 ”的工作原则，成立相应的领导及实施机构，结合本单位的实际情况，准确开展信息系统等级保护定级工作。 保监会成立等级保护定级工作领导小组，统一领导、解决保险行业信息安全等级保护定级工作中的重大问题；保监会等级保护定级工作领导小组下设办公室,具体负责保监会机关信息系统等级保护定级的具体实施工作和行业定级工作的指导审核。 各保监局负责本局内独立运行的信息系统等级保护定级工作，并对各自辖区内的保险公司分支机构的等级保护定级工作进行指导审核。 各保险集团公司、保险控股公司负责本公司信息系统等级保护定级工作以及其下属子公司信息系统等级保护定级工作的组织协调和指导。各保险总公司统一部署本公司和分公司的信息系统等级保护定级工作。 二、定级工作安排及定级范围 （一）定级工作安排 为稳妥做好等级保护定级工作，拟在保险行业内分步分批实

施。 保险行业第一批定级单位包括：保监会及各保监局，中国保险行业协会，中国人民保险集团公司、中国人寿保险（集团）公司、中国再保险（集团）公司、中国出口信用保险公司、民生人寿保险股份有限公司、阳光保险控股股份有限公司、中国平安保险（集团）股份有限公司、中国太平洋（集团）股份有限公司及其下属各子公司和分公司。 其余公司作为第二批定级单位（具体时间安排另行通知）。 （二）定级范围 1、保险监管部门监管、办公及网站等重要信息系统；保险公司和中国保险行业协会经营、治理、办公等重要信息系统。（以下简称“ 重要信息系统 ”） 2、涉及国家秘密的信息系统（以下简称“ 涉密信息系统 ”）。 三、主要工作步骤 第一阶段：自主定级（9月20日前完成） 各单位按要求成立相关定级实施机构，对本系统内的重要信息系统和涉密信息系统展开摸底调查，全面把握信息网络和信息系统的数量、分布、业务类型、系统结构、应用或服务范围等基本情况，按照《信息安全等级保护治理办法》（以下简称“ 《治理办法》 ”，附件1）和《信息系统安全等级保护定级指南》（附件2）的要求，确定定级对象并初步确定保护等级，形成定级报告（报告模板见附件3）。 涉密信息系统的等级确定按照国家保密局的有关规定和标准执行。 第二阶段：审核（9月25日前完成） 各保监局将各自独立运行的重要信息系统和涉密信息系统的定级报告报保监会审核。 各公司对本公司内的重要信息系统和涉密信息系统定级进行统一审核，对跨省联网运行且由公司总部统一确定等级的，由总公司将重要信息系统和涉密信息系统的定级报告报保监会审核 (有集团或控股公司的，由集团或控股公司将定级报告统一报保监会审

核)；保险公司分公司将经过总公司审核的，且在分公司独立运行的重要信息系统和涉密系统定级报告报当地保监局审核。 保险行业协会将所确定的重要信息系统和涉密信息系统的定级报告报保监会审核。 保监会及各保监局在接到定级报告审核文件后，对不符合要求的于5个工作日内要求其改正，审核通过者不再单独答复。 第三阶段：备案（9月30日前完成） 根据《治理办法》，各单位定级报告通过保监会或保监局审核后，对重要信息系统安全等级确定为二级以上的信息系统应到公安部网站下载《信息系统安全等级保护备案表》（见附件4）和辅助备案工具，并持填写的备案表和利用辅助备案工具生成的备案电子数据文件，到公安机关办理备案手续（保险行业协会确定的信息系统、保险总公司统一定级的跨省联网运营的信息系统，向公安部备案；保险公司分公司将总公司定级的跨省联网在当地运行、应用的分支系统以及在当地分公司独立运行的信息系统，向当地省级公安机关备案）。备案完成后，各级单位将备案证实复印件报相对应的保险监管机构存档。 涉密信息系统建设使用单位依据《治理办法》和国家保密局的有关规定，填写《涉及国家秘密的信息系统分级保护备案表》（见附件5），按照属地化治理原则，将所确定的涉密信息系统，报送相对应的保密部门备案。备案完成后，各级单位将备案证实复印件报相对应的保险监管机构存档。 第四阶段：总结工作（10月15日前完成） 各单位应对等级保护定级工作进行总结，并报保监会等级保护定级工作领导小组。保监会根据定级工作开展的情况和定级工作报告，总结工作经验，研究并启动第二批等级保护定级工作。 联 系 人：李春亮、王晓鹏 联系电话：010－66286602 附件：1

、信息安全等级保护治理办法 2、信息安全技术信息系统安全等级保护定级指南 3、信息系统安全等级保护定级报告 4、信息系统安全等级保护备案表 5、涉及国家秘密的信息系统分级保护备案表 二〇〇七年九月六日附件1：信息安全等级保护治理办法（公通字[2007]43号）第一章 总则 第一条 为规范信息安全等级保护治理，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，根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，制定本办法。 第二条 国家通过制定统一的信息安全等级保护治理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、治理。 第三条 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。国家密码治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。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治理。国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。 第四条 信息系统主管部门应当依照本办法及相关标准规范，督促、检查、指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。 第五条 信息系统的运营、使用单位应当依照本办法及其相关标准规范，履行信息安全等级保护的义务和责任。第二章 等级划分与保护 第六条 国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后

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等因素确定。 第七条 信息系统的安全保护等级分为以下五级：第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。 第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。 第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成非凡严重损害，或者对国家安全造成严重损害。 第五级，信息系统受到破坏后，会对国家安全造成非凡严重损害。 第八条 信息系统运营、使用单位依据本办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督治理。 第一级信息系统运营、使用单位应当依据国家有关治理规范和技术标准进行保护。 第二级信息系统运营、使用单位应当依据国家有关治理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行指导。 第三级信息系统运营、使用单位应当依据国家有关治理规范和技术标准进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行监督、检查。 第四级信息系统运营、使用单位应当依据国家有关治理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。 第五级信息系统运营、使用单位应当依据国家治理规范、技术标准和业务非凡安全需求进行保护。国家指定专门部

门对该级信息系统信息安全等级保护工作进行专门监督、检查。第三章 等级保护的实施与治理 第九条 信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作。 第十条 信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。有主管部门的，应当经主管部门审核批准。 跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。 对拟确定为第四级以上信息系统的，运营、使用单位或者主管部门应当请国家信息安全保护等级专家评审委员会评审。 第十一条 信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护治理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。 第十二条 在信息系统建设过程中，运营、使用单位应当按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）、《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术 数据库治理系统安全技术要求》（GB/T20273-2006）、《信息安全技术 服务器技术要求》、《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671 -2006）等技术标准同步建设符合该等级要求的信息安全设施。 第十三条 运营、使用单位应当参照《信息安全技术 信息系统安全治理要求》（GB/T20269-2006）、《信息安全技术 信息系统安全工程治

理要求》（GB/T20282-2006）、《信息系统安全等级保护基本要求》等治理规范，制定并落实符合本系统安全保护等级要求的安全治理制度。 第十四条 信息系统建设完成后，运营、使用单位或者其主管部门应当选择符合本办法规定条件的测评机构，依据《信息系统安全等级保护测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统应当每年至少进行一次等级测评，第四级信息系统应当每半年至少进行一次等级测评，第五级信息系统应当依据非凡安全需求进行等级测评。 信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行自查。第三级信息系统应当每年至少进行一次自查，第四级信息系统应当每半年至少进行一次自查，第五级信息系统应当依据非凡安全需求进行自查。 经测评或者自查，信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改。 第十五条 已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。 新建第二级以上信息系统，应当在投入运行后30日内，由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。 隶属于中心的在京单位，其跨省或者全国统一联网运行并由主管部门统一定级的信息系统，由主管部门向公安部办理备案手续。跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应当向当地设区的市级以上公安机关备案。 第十六条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：（

一）系统拓扑结构及说明；（二）系统安全组织机构和治理制度；（三）系统安全保护设施设计实施方案或者改建实施方案；（四）系统使用的信息安全产品清单及其认证、销售许可证实；（五）测评后符合系统安全保护等级的技术检测评估报告；（六）信息系统安全保护等级专家评审意见；（七）主管部门审核批准信息系统安全保护等级的意见。 第十七条 信息系统备案后，公安机关应当对信息系统的备案情况进行审核，对符合等级保护要求的，应当在收到备案材料之日起的10个工作日内颁发信息系统安全等级保护备案证实；发现不符合本办法及有关标准的，应当在收到备案材料之日起的10个工作日内通知备案单位予以纠正；发现定级不准的，应当在收到备案材料之日起的10个工作日内通知备案单位重新审核确定。 运营、使用单位或者主管部门重新确定信息系统等级后，应当按照本办法向公安机关重新备案。 第十八条 受理备案的公安机关应当对第三级、第四级信息系统的运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次，对第四级信息系统每半年至少检查一次。对跨省或者全国统一联网运行的信息系统的检查，应当会同其主管部门进行。 对第五级信息系统，应当由国家指定的专门部门进行检查。 公安机关、国家指定的专门部门应当对下列事项进行检查：（一）信息系统安全需求是否发生变化，原定保护等级是否准确；（二）运营、使用单位安全治理制度、措施的落实情况；（三）运营、使用单位及其主管部门对信息系统安全状况的检查情况；（四）系统安全等级测评是否符合要求；（五）信息安全产品使用是否符合要求；（六）信息系统安全整改情况；（七）备案材

料与运营、使用单位、信息系统的符合情况；（八）其他应当进行监督检查的事项。 第十九条 信息系统运营、使用单位应当接受公安机关、国家指定的专门部门的安全监督、检查、指导，如实向公安机关、国家指定的专门部门提供下列有关信息安全保护的信息资料及数据文件：（一）信息系统备案事项变更情况；（二）安全组织、人员的变动情况；（三）信息安全治理制度、措施变更情况；（四）信息系统运行状况记录；（五）运营、使用单位及主管部门定期对信息系统安全状况的检查记录；（六）对信息系统开展等级测评的技术测评报告；（七）信息安全产品使用的变更情况；（八）信息安全事件应急预案，信息安全事件应急处置结果报告；（九）信息系统安全建设、整改结果报告。 第二十条 公安机关检查发现信息系统安全保护状况不符合信息安全等级保护有关治理规范和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求，按照治理规范和技术标准进行整改。整改完成后，应当将整改报告向公安机关备案。必要时，公安机关可以对整改情况组织检查。 第二十一条 第三级以上信息系统应当选择使用符合以下条件的信息安全产品：（一）产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；（二）产品的核心技术、要害部件具有我国自主知识产权；（三）产品研制、生产单位及其主要业务、技术人员无犯罪记录；（四）产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；（五）对国家安全、社会秩序、公共利益不构成危害；（六）对已列入信息安全产品认证目录的，应当取得国家

信息安全产品认证机构颁发的认证证书。 第二十二条 第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：（一）在中华人民共和国境内注册成立（港澳台地区除外）；（二）由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；（三）从事相关检测评估工作两年以上，无违法记录；（四）工作人员仅限于中国公民；（五）法人及主要业务、技术人员无犯罪记录；（六）使用的技术装备、设施应当符合本办法对信息安全产品的要求；（七）具有完备的保密治理、项目治理、质量治理、人员治理和培训教育等安全治理制度；（八）对国家安全、社会秩序、公共利益不构成威胁。 第二十三条 从事信息系统安全等级测评的机构，应当履行下列义务：（一）遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；（二）保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；（三）对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。第四章 涉及国家秘密信息系统的分级保护治理 第二十四条 涉密信息系统应当依据国家信息安全等级保护的基本要求，按照国家保密工作部门有关涉密信息系统分级保护的治理规定和技术标准，结合系统实际情况进行保护。非涉密信息系统不得处理国家秘密信息。 第二十五条 涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密三个等级。 涉密信息系统建设使用单位应当在信息规范定密的基础上，依据涉密信息系统分级保护治理办法和国家保密标准BMB17-2006《涉及国家秘密的计算机信息系

统分级保护技术要求》确定系统等级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定保护等级。 保密工作部门和机构应当监督指导涉密信息系统建设使用单位准确、合理地进行系统定级。 第二十六条 涉密信息系统建设使用单位应当将涉密信息系统定级和建设使用情况，及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。 第二十七条 涉密信息系统建设使用单位应当选择具有涉密集成资质的单位承担或者参与涉密信息系统的设计与实施。 涉密信息系统建设使用单位应当依据涉密信息系统分级保护治理规范和技术标准，按照秘密、机密、绝密三级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上不低于国家信息安全等级保护第三级、第四级、第五级的水平。 第二十八条 涉密信息系统使用的信息安全保密产品原则上应当选用国产品，并应当通过国家保密局授权的检测机构依据有关国家保密标准进行的检测，通过检测的产品由国家保密局审核发布目录。 第二十九条 涉密信息系统建设使用单位在系统工程实施结束后，应当向保密工作部门提出申请，由国家保密局授权的系统测评机构依据国家保密标准BMB22-2007《涉及国家秘密的计算机信息系统分级保护测评指南》，对涉密信息系统进行安全保密测评。 涉密信息系统建设使用单位在系统投入使用前，应当按照《涉及国家秘密的信息系统审批治理规定》，向设区的市级以上保密工作部门申请进行系统审批，涉密信息系统通过审批后方可投入使用。已投入使用的涉密信息系统，其建设使用单位在按照分级保护要求完成系统整改后，应当向保密工作部门备案。 第三十条 涉密信

息系统建设使用单位在申请系统审批或者备案时，应当提交以下材料：（一）系统设计、实施方案及审查论证意见；（二）系统承建单位资质证实材料；（三）系统建设和工程监理情况报告；（四）系统安全保密检测评估报告；（五）系统安全保密组织机构和治理制度情况；（六）其他有关材料。第三十一条 涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密治理责任单位变更时，其建设使用单位应当及时向负责审批的保密工作部门报告。保密工作部门应当根据实际情况，决定是否对其重新进行测评和审批。第三十二条 涉密信息系统建设使用单位应当依据国家保密标准BMB20-2007《涉及国家秘密的信息系统分级保护治理规范》，加强涉密信息系统运行中的保密治理，定期进行风险评估，消除泄密隐患和漏洞。第三十三条 国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督治理，并做好以下工作：（一）指导、监督和检查分级保护工作的开展；（二）指导涉密信息系统建设使用单位规范信息定密，合理确定系统保护等级；（三）参与涉密信息系统分级保护方案论证，指导建设使用单位做好保密设施的同步规划设计；（四）依法对涉密信息系统集成资质单位进行监督治理；（五）严格进行系统测评和审批工作，监督检查涉密信息系统建设使用单位分级保护治理制度和技术措施的落实情况；（六）加强涉密信息系统运行中的保密监督检查。对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评，对绝密级信息系统每年至少进行一次保密检查或者系统测评；（七）了解把握各级各类涉密信息系统的治理使用情况，及时发现和查处各种违规违法行为

和泄密事件。 第五章 信息安全等级保护的密码治理 第三十四条 国家密码治理部门对信息安全等级保护的密码实行分类分级治理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。 信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护密码治理办法》、《信息安全等级保护商用密码技术要求》等密码治理规定和相关标准。 第三十五条 信息系统安全等级保护中密码的配备、使用和治理等，应当严格执行国家密码治理的有关规定。 第三十六条 信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码治理局审批，密码的设计、实施、使用、运行维护和日常治理等，应当按照国家密码治理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码治理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码治理机构备案。 第三十七条 运用密码技术对信息系统进行系统等级保护建设和整改的，必须采用经国家密码治理部门批准使用或者准于销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。 第三十八条 信息系统中的密码及密码设备的测评工作由国家密码治理局认可的测评机构承担，其他任何部门、单位和个人不得对密码进行评测和监控。 第三十九条 各级密码治理部门可以定期或者不定期对信息系统等级保护工

作中密码配备、使用和治理的情况进行检查和测评，对重要涉密信息系统的密码配备、使用和治理情况每两年至少进行一次检查和测评。在监督检查过程中，发现存在安全隐患或者违反密码治理相关规定或者未达到密码相关标准要求的，应当按照国家密码治理的相关规定进行处置。 第六章 法律责任 第四十条 第三级以上信息系统运营、使用单位违反本办法规定，有下列行为之一的，由公安机关、国家保密工作部门和国家密码工作治理部门按照职责分工责令其限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况，建议对其直接负责的主管人员和其他直接责任人员予以处理，并及时反馈处理结果：（一）未按本办法规定备案、审批的；（二）未按本办法规定落实安全治理制度、措施的；（三）未按本办法规定开展系统安全状况检查的；（四）未按本办法规定开展系统安全技术测评的；（五）接到整改通知后，拒不整改的；（六）未按本办法规定选择使用信息安全产品和测评机构的；（七）未按本办法规定如实提供有关文件和证实材料的；（八）违反保密治理规定的；（九）违反密码治理规定的；（十）违反本办法其他规定的。 违反前款规定，造成严重损害的，由相关部门依照有关法律、法规予以处理。 第四十一条 信息安全监管部门及其工作人员在履行监督治理职责中，玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。第七章 附则 第四十二条 已运行信息系统的运营、使用单位自本办法施行之日起180日内确定信息系统的安全保护等级；新建信息系统在设计、规划阶段确定安全保护等级。 第四十三条 本办法所称“ 以上 ”包含本数（级）。 第四十四条 本办法自发布之日

起施行，《信息安全等级保护治理办法（试行）》（公通字[2006]7号）同时废止。附件2：信息安全技术信息系统安全等级保护定级指南（报批稿）全国信息安全标准化技术委员会 前 言本标准由公安部和全国信息安全标准化技术委员会提出。本标准由全国信息安全标准化技术委员会归口。本标准起草单位：本标准主要起草人：引 言依据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《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）、《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）和《信息安全等级保护治理办法》（公通字[2007]43号），制定本标准。本标准是信息安全等级保护相关系列标准之一。与本标准相关的系列标准包括：GB/T BBBBB-BBBB信息系统安全等级保护基本要求；GB/T CCCCC-CCCC信息系统安全等级保护实施指南；GB/T DDDDD-DDDD信息系统安全等级保护测评准则。本标准依据等级保护相关治理文件，从信息系统所承载的业务在国家安全、经济建设、社会生活中的重要作用和业务对信息系统的依靠程度这两方面，提出确定信息系统安全保护等级的方法。 信息系统安全等级保护定级指南1范围本标准规定了信息系统安全等级保护的定级方法，适用于为信息系统安全等级保护的定级工作提供指导。2规范性引用文件下列文件中的条款通过在本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。GB/T 5271.8 信息技

术 词汇 第8部分：安全 GB17859-1999 计算机信息系统安全保护等级划分准则3术语和定义GB/T 5271.8和GB17859-1999确立的以及下列术语和定义适用于本标准。3.1等级保护对象 target of classified security信息安全等级保护工作直接作用的具体的信息和信息系统。3.2客体object受法律保护的、等级保护对象受到破坏时所侵害的社会关系，如国家安全、社会秩序、公共利益以及公民、法人或其他组织的合法权益。3.3客观方面objective 对客体造成侵害的客观外在表现，包括侵害方式和侵害结果等。3.4系统服务 system service信息系统为支撑其所承载业务而提供的程序化过程。4定级原理4.1信息系统安全保护等级根据等级保护相关治理文件，信息系统的安全保护等级分为以下五级：第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成非凡严重损害，或者对国家安全造成严重损害。第五级，信息系统受到破坏后，会对国家安全造成非凡严重损害。4.2信息系统安全保护等级的定级要素信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。4.2.1受侵害的客体等级保护对象受到破坏时所侵害的客体包括以下三个方面：a)公民、法人和其他组织的合法权益；b)社会秩序、公共利益；c)国家安全。4.2.2对客体的侵害

程度对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：a)造成一般损害；b)造成严重损害；c)造成非凡严重损害。4.3定级要素与等级的关系定级要素与信息系统安全保护等级的关系如表1所示。表1 定级要素与安全保护等级的关系受侵害的客体对客体的侵害程度一般损害严重损害非凡严重损害公民、法人和其他组织的合法权益第一级第二级第二级社会秩序、公共利益第二级第三级第四级国家安全第三级第四级第五级5定级方法5.1定级的一般流程信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的信息系统安全保护等级称业务信息安全保护等级。从系统服务安全角度反映的信息系统安全保护等级称系统服务安全保护等级。确定信息系统安全保护等级的一般流程如下：a)确定作为定级对象的信息系统；b)确定业务信息安全受到破坏时所侵害的客体；c)根据不同的受侵害客体，从多个方面综合评定业务信息安全被破坏对客体的侵害程度；d)依据表2，得到业务信息安全保护等级；e)确定系统服务安全受到破坏时所侵害的客体；f)根据不同的受侵害客体，从多个方面综合评定系统服务安全被破坏对客体的侵害程度；g)依据表3，得到系统服务安全保护等级；h)将业务信息安全保护等级和系统服务安全保护等级的较高者确定为定级对象的安全保护等级。上

述步骤如图1确定等级一般流程所示。 图1 确定等级一般流程5.2确定定级对象一个单位内运行的信息系统可能比较庞大，为了体现重要部分重点保护，有效控制信息安全建设成本，优化信息安全资源配置的等级保护原则，可将较大的信息系统划分为若干个较小的、可能具有不同安全保护等级的定级对象。作为定级对象的信息系统应具有如下基本特征：a)具有唯一确定的安全责任单位作为定级对象的信息系统应能够唯一地确定其安全责任单位。假如一个单位的某个下级单位负责信息系统安全建设、运行维护等过程的全部安全责任，则这个下级单位可以成为信息系统的安全责任单位；假如一个单位中的不同下级单位分别承担信息系统不同方面的安全责任，则该信息系统的安全责任单位应是这些下级单位共同所属的单位。b)具有信息系统的基本要素作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的有形实体。应避免将某个单一的系统组件，如服务器、终端、网络设备等作为定级对象。c)承载单一或相对独立的业务应用定级对象承载“单一”的业务应用是指该业务应用的业务流程独立，且与其他业务应用没有数据交换，且独享所有信息处理设备。定级对象承载“相对独立”的业务应用是指其业务应用的主要业务流程独立，同时与其他业务应用有少量的数据交换，定级对象可能会与其他业务应用共享一些设备，尤其是网络传输设备。5.3确定受侵害的客体定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。侵害国家安全的事项包括以下方面：-影响国家政权稳固和国防实力；-影响国家统一、民族团结和社会安定；-影

响国家对外活动中的政治、经济利益；-影响国家重要的安全保卫工作；-影响国家经济竞争力和科技实力；-其他影响国家安全的事项。侵害社会秩序的事项包括以下方面：-影响国家机关社会治理和公共服务的工作秩序；-影响各种类型的经济活动秩序；-影响各行业的科研、生产秩序；-影响公众在法律约束和道德规范下的正常生活秩序等；-其他影响社会秩序的事项。影响公共利益的事项包括以下方面：-影响社会成员使用公共设施；-影响社会成员获取公开信息资源；-影响社会成员接受公共服务等方面；-其他影响公共利益的事项。影响公民、法人和其他组织的合法权益是指由法律确认的并受法律保护的公民、法人和其他组织所享有的一定的社会权利和利益。确定作为定级对象的信息系统受到破坏后所侵害的客体时，应首先判定是否侵害国家安全，然后判定是否侵害社会秩序或公众利益，最后判定是否侵害公民、法人和其他组织的合法权益。各行业可根据本行业业务特点，分析各类信息和各类信息系统与国家安全、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关系，从而确定本行业各类信息和各类信息系统受到破坏时所侵害的客体。5.4确定对客体的侵害程度5.4.1侵害的客观方面在客观方面，对客体的侵害外在表现为对定级对象的破坏，其危害方式表现为对信息安全的破坏和对信息系统服务的破坏，其中信息安全是指确保信息系统内信息的保密性、完整性和可用性等，系统服务安全是指确保信息系统可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种危害方式。信息安全

和系统服务安全受到破坏后，可能产生以下危害后果：-影响行使工作职能；-导致业务能力下降；-引起法律纠纷；-导致财产损失；-造成社会不良影响；-对其他组织和个人造成损失；-其他影响。5.4.2综合判定侵害程度侵害程度是客观方面的不同外在表现的综合体现，因此，应首先根据不同的受侵害客体、不同危害后果分别确定其危害程度。对不同危害后果确定其危害程度所采取的方法和所考虑的角度可能不同，例如系统服务安全被破坏导致业务能力下降的程度可以从信息系统服务覆盖的区域范围、用户人数或业务量等不同方面确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。在针对不同的受侵害客体进行侵害程度的判定时，应参照以下不同的判别基准：-假如受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判定侵害程度的基准；-假如受侵害客体是社会秩序、公共利益或国家安全，则应以整个行业或国家的总体利益作为判定侵害程度的基准。不同危害后果的三种危害程度描述如下：一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害。严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。非凡严重损害：工作职能受到非凡严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组

织和个人造成非常严重损害。信息安全和系统服务安全被破坏后对客体的侵害程度，由对不同危害结果的危害程度进行综合评定得出。由于各行业信息系统所处理的信息种类和系统服务特点各不相同，信息安全和系统服务安全受到破坏后关注的危害结果、危害程度的计算方式均可能不同，各行业可根据本行业信息特点和系统服务特点，制定危害程度的综合评定方法，并给出侵害不同客体造成一般损害、严重损害、非凡严重损害的具体定义。5.5确定定级对象的安全保护等级根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表2业务信息安全保护等级矩阵表，即可得到业务信息安全保护等级。表2 业务信息安全保护等级矩阵表业务信息安全被破坏时所侵害的客体对相应客体的侵害程度一般损害严重损害非凡严重损害公民、法人和其他组织的合法权益第一级第二级第二级社会秩序、公共利益第二级第三级第四级国家安全第三级第四级第五级根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表2系统服务安全保护等级矩阵表，即可得到系统服务安全保护等级。表3 系统服务安全保护等级矩阵表系统服务安全被破坏时所侵害的客体对相应客体的侵害程度一般损害严重损害非凡严重损害公民、法人和其他组织的合法权益第一级第二级第二级社会秩序、公共利益第二级第三级第四级国家安全第三级第四级第五级作为定级对象的信息系统的安全保护等级由业务信息安全保护等级和系统服务安全保护等级的较高者决定。6等级变更在信息系统的运行过程中，安全保护等级应随着信息系统所处理的信息和业务状态的变化进行适当的变更，尤其是当状态变化可能导致业务信息安全或系统服务

受到破坏后的受侵害客体和对客体的侵害程度有较大的变化，可能影响到系统的安全保护等级时，应根据本标准第5章给出的定级方法重新定级。附件3：信息系统安全等级保护定级报告一、XXX信息系统描述简述确定该系统为定级对象的理由。从三方面进行说明：一是描述承担信息系统安全责任的相关单位或部门，说明本单位或部门对信息系统具有信息安全保护责任，该信息系统为本单位或部门的定级对象；二是该定级对象是否具有信息系统的基本要素，描述基本要素、系统网络结构、系统边界和边界设备；三是该定级对象是否承载着单一或相对独立的业务，业务情况描述。二、XXX信息系统安全保护等级确定（定级方法参见国家标准《信息系统安全等级保护定级指南》）（一）业务信息安全保护等级的确定1、业务信息描述描述信息系统处理的主要业务信息等。2、业务信息受到破坏时所侵害客体的确定说明信息受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。3、信息受到破坏后对侵害客体的侵害程度的确定说明信息受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是非凡严重损害。4、业务信息安全等级的确定依据信息受到破坏时所侵害的客体以及侵害程度，确定业务信息安全等级。（二）系统服务安全保护等级的确定1、系统服务描述描述信息系统的服务范围、服务对象等。2、系统服务受到破坏时所侵害客体的确定说明系统服务受到破坏时侵害的客体是什么，即对三个客体（国家安全；社会秩序和公众利益；公民、法人和其他组织的合法权益）中的哪些客体造成侵害。3、系统服务受到破坏后

对侵害客体的侵害程度的确定说明系统服务受到破坏后，会对侵害客体造成什么程度的侵害，即说明是一般损害、严重损害还是非凡严重损害。4、系统服务安全等级的确定依据系统服务受到破坏时所侵害的客体以及侵害程度确定系统服务安全等级。（三）安全保护等级的确定信息系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定，最终确定XXX系统安全保护等级为第几级。信息系统名称安全保护等级业务信息安全等级系统服务安全等级XXX信息系统XXX附件4：备案表编号：信息系统安全等级保护备案表备案 单 位：（盖章） 备 案 日 期： 受理备案单位：（盖章） 受 理 日 期： 中华人民共和国公安部监制 填 表 说 明一、制表依据。根据《信息安全等级保护治理办法》（公通字[2007]43号）之规定，制作本表；二、填表范围。本表由第二级以上信息系统运营使用单位或主管部门（以下简称“ 备案单位 ”）填写；本表由四张表单构成，表一为单位信息，每个填表单位填写一张；表二为信息系统基本信息，表三为信息系统定级信息，表二、表三每个信息系统填写一张；表四为第三级以上信息系统需要同时提交的内容，由每个第三级以上信息系统填写一张，并在完成系统建设、整改、测评等工作，投入运行后三十日内向受理备案公安机关提交；表二、表三、表四可以复印使用；三、保存方式。本表一式二份，一份由备案单位保存，一份由受理备案公安机关存档；四、本表中有选择的地方请在选项左侧“ 0 ”划“ √ ”，如选择“ 其他 ”，请在其后的横线中注明具体内容；五、封面中备案表编号（由受理备案的公安机关填写并校验）：分两部分共11位，第一部分6位，为受理备案公安机关代码前六位（

可参照行标GA380-2002）。第二部分5位，为受理备案的公安机关给出的备案单位的顺序编号；六、封面中备案单位：是指负责运营使用信息系统的法人单位全称；七、封面中受理备案单位：是指受理备案的公安机关公共信息网络安全监察部门名称。此项由受理备案的公安机关负责填写并盖章；八、表一04行政区划代码：是指备案单位所在的地(区、市、州、盟)行政区划代码；九、表一05单位负责人：是指主管本单位信息安全工作的领导；十、表一06责任部门：是指单位内负责信息系统安全工作的部门；十一、表一08隶属关系：是指信息系统运营使用单位与上级行政机构的从属关系，须按照单位隶属关系代码（GB/T12404—1997）填写；十二、表二02系统编号：是由运营使用单位给出的本单位备案信息系统的编号；十三、表二05系统网络平台：是指系统所处的网络环境和网络构架情况；十四、表二07要害产品使用情况：国产品是指系统中该类产品的研制、生产单位是由中国公民、法人投资或者国家投资或者控股，在中华人民共和国境内具有独立的法人资格，产品的核心技术、要害部件具有我国自主知识产权；十五、表二08系统采用服务情况：国内服务商是指服务机构在中华人民共和国境内注册成立（港澳台地区除外），由中国公民、法人或国家投资的企事业单位；十六、表三01、02、03项：填写上述三项内容，确定信息系统安全保护等级时可参考《信息系统安全等级保护定级指南》，信息系统安全保护等级由业务信息安全等级和系统服务安全等级较高者决定。01、02项中每一个确定的级别所对应的损害客体及损害程度可多选；十七、表三06主管部门：是指对备案单位信息系统负领导责任的行政或业务主管单位或部

门。部级单位此项可不填；十八、解释：本表由公安部公共信息网络安全监察局监制并负责解释，未经答应，任何单位和个人不得对本表进行改动。 表一 单位基本情况01单位名称02单位地址 省(自治区、直辖市) 地(区、市、州、盟) 县(区、市、旗)03邮政编码04行政区划代码05单位负责人姓 名职务/职称办公电话电子邮件06责任部门07责任部门联系人姓 名职务/职称办公电话电子邮件移动电话08隶属 关系01中心 02省(自治区、直辖市) 03地(区、市、州、盟)04县（区、市、旗） 09其他 09单位类型01党委机关 02政府机关 03事业单位 04企业 09其他 10行业类别011电信 012广电 013经营性公众互联网021铁路 022银行 023海关 024税务 025民航 026电力 027证券 028保险031国防科技工业 032公安 033人事劳动和社会保障 034财政035审计 036商业贸易 037国土资源 038能源039交通 040统计 041工商行政治理 042邮政043教育 044文化 045卫生 046农业 047水利 048外交 049发展改革 050科技 051宣传 052质量监督检验检疫099其他 11信息系统总数 个12第二级信息系统数个13第三级信息系统数个14第四级信息系统数个15第五级信息系统数个 表二（ / ）信息系统情况01系统名称02系统编号03统承载业务情况业务类型01生产作业 02指挥调度 03治理控制 04内部办公 05公众服务 09其他 业务描述04系统服务情况服务范围010全国 011跨省（区、市） 跨 个 020全省（区、市） 021跨地（市、区） 跨 个030地（市、区）内 099其它 服务对象01单位内部人员 02社会公众人员 03两者均包括 09其他 05系统网络平台覆盖范围01局域网 02城域网 03广域网 09其他 网络性质01业务专网 02互联网 09其它 06系统互联情况01与其他行业系统连接 02与本行业其他单位系统连接03与本单位其他系统连接

09其它 07要害产品使用情况序号产品类型数量使用国产品率 全部使用 全部未使用部分使用及使用率 1安全专用产品000 %2网络产品000 %3操作系统000 %4数据库000 %5服务器000 %6其他 000 %08系统采用服务情况序号服务类型服务责任方类型本行业（单位）国内其他服务商国外服务商1等级测评0有0无0002风险评估0有0无0003灾难恢复0有0无0004应急响应0有0无0005系统集成0有0无0006安全咨询0有0无0007安全培训0有0无0008其它 00009等级测评单位名称10何时投入运行使用 年 月 日11系统是否是分系统0是 0否（如选择是请填下两项）12上级系统名称13上级系统所属单位名称 表三（ / ）信息系统定级情况01确定业务信息安全保护等级损害客体及损害程度级别0仅对公民、法人和其他组织的合法权益造成损害0第一级0对公民、法人和其他组织的合法权益造成严重损害0对社会秩序和公共利益造成损害0第二级0对社会秩序和公共利益造成严重损害0对国家安全造成损害0第三级0对社会秩序和公共利益造成非凡严重损害0对国家安全造成严重损害0第四级0对国家安全造成非凡严重损害0第五级02确定系统服务安全保护等级0仅对公民、法人和其他组织的合法权益造成损害0第一级0对公民、法人和其他组织的合法权益造成严重损害0对社会秩序和公共利益造成损害0第二级0对社会秩序和公共利益造成严重损害0对国家安全造成损害0第三级0对社会秩序和公共利益造成非凡严重损害0对国家安全造成严重损害0第四级0对国家安全造成非凡严重损害0第五级03信息系统安全保护等级0第一级 0第二级 0第三级 0第四级 0第五级04定级时间 年 月 日05专家评审情况0已评审 0未评审06是否有主管部门0有 0无（如选择有请填下两项）07主管部门名称08主管部

门审批定级情况0已审批 0未审批09系统定级报告0有 0无 附件名称 填表人： 填表日期： 年 月 日备案审核民警： 审核日期： 年 月 日 表四（ / ）第三级以上信息系统提交材料情况01系统拓扑结构及说明0有 0无 附件名称 02系统安全组织机构及治理制度0有 0无 附件名称 03系统安全保护设施设计实施方案或改建实施方案0有 0无 附件名称 04系统使用的安全产品清单及认证、销售许可证实0有 0无 附件名称 05系统等级测评报告0有 0无 附件名称 06专家评审情况0有 0无 附件名称 07上级主管部门审批意见0有 0无 附件名称 附件5： 单位名称涉密信息系统名称系统密级（保护等级）□ 秘密 □ 机密 □ 绝密系统联接范围□局域网 □城域网 □广域网（跨 个省或地）系统安全域划分和安全域密级确定□未划分安全域□划分安全域（共有 个，其中绝密级 个， 机密级 个，秘密级 个，内部级 个）系统主要承建单位系统投入使用时间系统运行治理部门系统安全保密治理部门系统分级保护实施情况□已经实施 □正在实施 □计划 年实施 涉及国家秘密的信息系统分级保护备案表填报日期： 年 月 日 填报单位：（盖章）填表说明：1. “ 系统密级 ”依据《涉及国家秘密的信息系统分级保护治理办法》和国家保密标准BMB17-2006确定。2. 涉密信息系统一般应划分安全域，同一系统内的不同安全域根据所处理信息的重要程度，可分别确定密级。3. 表中“ □ ”项，确认划“ √ ”。4. 填报多个涉密信息系统，可复印此表。国家保密局制 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com