信息系统定级与备案工作介绍

本文主要介绍信息系统安全保护等级的确定，定级工作的流程和要求，备案工作的流程和要求等。

一、信息系统安全保护等级的划分与保护

（一）信息系统定级工作原则

信息系统定级工作应按照“自主定级、专家评审、主管部门审批、公安机关审核”的原则进行。定级工作的主要内容包括：确定定级对象、确定信息系统安全保护等 级、组织专家评审、主管部门审批、公安机关审核。各信息系统运营使用单位和主管部门是信息安全等级保护的责任主体，根据所属信息系统的重要程度和遭到破坏后的危害程度，确定信息系统的安全保护 等级。同时，按照所定等级，依照相应等级的管理规范和技术标准，建设信息安全保护设施，建立安全制度，落实安全责任，对信息系统进行保护。

在等级保护工作中，信息系统运营使用单位和主管部门按照“谁主管谁负责，谁运营谁负责”的原则开展工作，并接受信息安全监管部门对开展等级保护工作的监管。 运营使用单位和主管部门是信息系统安全的第一责任人，对所属信息系统安全负有直接责任；公安、保密、密码部门对运营使用单位和主管部门开展等级保护工作进 行监督、检查、指导，对重要信息系统安全负监管责任。由于重要信息系统的安全运行不仅影响本行业、本单位的生产和工作秩序，也会影响国家安全、社会稳定、 公共利益，因此，国家必然要对重要信息系统的安全进行监管。

（二）信息系统安全保护等级

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，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。信息系统的安全保护等级分为五级，从第一级到第五级逐级增高。

（三）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。

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：一是公民、法人和其他组织的合法权益；二是社会秩序、公共利益；三是国家安全。

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有三种：一是造成一般损害；二是造成严重损害；三是造成特别 严重损害。

（四）五级保护和监管

信息系统运营、使用单位依据国家信息安全等级保护政策和相关技术标准对信息系统进行保护，国家信息安全监管部门对其信息安全等级保护工作进行监督管理。定级要素与信息系统安全保护等级的关系如表 1-1 所示。

表 1-1 定级要素与安全保护等级的关系

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查

二、定级工作的主要步骤

信息系统定级是等级保护工作的首要环节和关键环节，是开展信息系统备案、建设整改、等级测评、监督检查等工作的重要基础。这里先明确一个概念，信息系统包括 起支撑、传输作用的基础信息网络和各类应用系统。信息系统安全级别定级不准，系统备案、建设整改、等级测评等后续工作都会失去基础，信息系统安全就没有保 证。定级工作可以按照下列步骤进行。

（一）开展摸底调查

按照《定级工作通知》确定的定级范围，各单位、各部门可以组织开展对所属信息系统进行摸底调查，摸清信息系统底数，掌握信息系统（包括信息网络）的业务类型、应用或服务范围、系统结构等基本情况，为下一步明确要求、落实责任奠定基础。

（二）确定定级对象

在全国重要信息系统安全等级保护定级工作（以下简称“定级工作”）中，如何科学、合理地确定定级对象是最关键的问题。信息系统运营使用单位或主管部门按如下原则确定定级对象。

一是起支撑、传输作用的信息网络（包括专网、内网、外网、网管系统）要作为定级对象。但不是将整个网络作为一个定级对象，而是要从安全管理和安全责任的角度将基础信息网络划分成若干个最小安全域或最小单元去定级。

二是用于生产、调度、管理、作业、指挥、办公等目的的各类业务系统，要按照不同业务类别单独确定为定级对象，不以系统是否进行数据交换、是否独享设备为确定定级对象条件。不能将某一类信息系统作为一个定级对象去定级。

三是各单位网站要作为独立的定级对象。如果网站的后台数据库管理系统安全级别高，也要作为独立的定级对象。网站上运行的信息系统（例如对社会服务的报名考试系统）也要作为独立的定级对象。

四是确认负责定级的单位是否对所定级系统负有业务主管责任。也就是说，业务部门应主导对业务信息系统定级，运维部门（例如信息中心、托管方）可以协助定级并按照业务部门的要求开展后续安全保护工作。

五是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。

例如，奥运网络主要包括，“奥组委办公外网”（承载自动化办公、场馆管理、电子邮件、物流、员工之家等 16 项业务）、“奥组委内部办公局域网”（承载着财务管理、人事管理等 3 项业务）、“奥运票务网”（票务网站和票务管理系统）、“奥运官方网站”（门户网站和后台数据处理系统）、“奥运互联网接入”、“竞赛网”等六个奥运信息系统。确定奥组委办公外网、奥组委内部办公局域网、票务网站、票务管理系统、奥运官方网站和竞赛网为定级对象。

（三）初步确定信息系统等级

可以按照下列要求确定信息系统等级：

1.定级责任主体。各信息系统运营使用单位和主管部门是信息系统定级的责任主体。

2.定级要素。信息系统的安全保护等级由两个定级的要素决定：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。

信息系统的安全保护等级是信息系统本身的客观自然属性，不以已采取或将采取什么安全保护措施为依据，而是以信息系统的重要性和信息系统遭到破坏后对国家安 全、社会稳定、人民群众合法公益的危害程度为依据，确定信息系统的安全保护等级。定级时应主要考虑信息系统破坏后对国家安全、社会稳定的影响，考虑境内外 各种敌对势力、敌对分子针对重要信息系统入侵攻击破坏和窃取秘密等因素。既要防止个别单位版面追求绝对安全而定级过高，也要防止为了逃避监管定级偏低。

3.对各类系统定级的处理方法。一是单位自建的信息系统（与上级单位无关），单位自主定级。二是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。其中：由各行业统一规划、统一建设、统一安全保护策略的全国联网系统，应由行业主管部门统一对下各级系统分别确定等级；由各行业统一规划、分 级建设、全国联网的信息系统，

应由部、省、地市分别确定系统等级，但各行业主管部门应对该系统提出定级意见，避免出现同类系统下级定级比上级高的现象。对 于该类系统的等级，下级确定后需报上级主管部门审批。

需特别注意的是：同类信息系统的安全保护等级不能随着部、省、市行政级别的降低而降低，例如地市级的重要行业的重要系统不能定为一、二级。

4.新建系统的定级工作

对于新建系统，信息系统运营使用单位在规划设计时应确定信息系统安全保护等级，按照信息系统等级，同步规划、同步设计、同步实施安全保护技术措施和管理措施。有关信息系统安全保护等级确定的具体办法和要求见 1.3 节。

（四）信息系统等级评审

信息系统运营使用单位或主管部门在初步确定信息系统安全保护等级后，为了保证定级合理、准确，可以聘请专家进行评审，并出具专家评审意见。

（五）信息系统等级的审批

单位自建的信息系统（与上级单位无关），等级确定后，是否报上级主管部门审批，由各行业自行决定。信息系统运营使用单位参考专家定级评审意见，最终确定信息 系统等级，形成《定级报告》。如果专家评审意见与运营使用单位意见不一致时，由运营使用单位自主决定系统等级，信息系统运营使用单位有上级主管部门的，应 当经上级主管部门对安全保护等级进行审核批准。主管部门一般是指行业的上级主管部门或监管部门。如果是跨地域联网运营使用的信息系统，则必须由其上级主管 部门审批，确保同类系统或分支系统在各地域分别定级的一致性。

（六）公安机关审核

公安机关收到信息系统运营使用单位备案材料后，应对信息系统定级的准确性进行审核。公安机关的审核是定级工作的最后一道防线，应予以高度重视，严格把关。信 息系统定级基本准确的，公安机关颁发由公安部统一监制的《信息系统安全等级保护备案证明》（以下简称《备案证明》）。对于定级不准的，公安机关应向备案单 位发整改通知，并建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。备案单位仍然坚持原定等级的，公安机关可以受理其备案，但应当书面告知其 承担由此引发的责任和后果，经上级公安机关同意后，同时通报备案单位上级主管部门。

三、如何确定信息系统安全保护等级

（一）如何理解信息系统的五个安全保护等级

信息系统的安全保护等级是信息系统的客观属性，不以已采取或将采取什么安全保护措施为依据，而是以信息系统的重要性和信息系统遭到破坏后对国家安全、社会稳 定、人民群众合法权益的危害程度为依据，确定信息系统的安全保护等级。既要防止个别单位片面追求绝对安全而定级过高，也要防止为了逃避监管定级偏低。信息 网络的安全等级可以参照在其上运行的信息系统的等级、网络的服务范围和自身的安全需求确定适当的保护等级，不以在其上运行的信息系统的最高等级或最低等级 为标准，既不就高、不就低。

为了帮助信息系统运营使用单位准确确定信息系统安全保护等级，可以参考下列对五级的说明确定系统等级。

第一级信息系统：一般适用于小型私营、个体企业、中小学，乡镇所属信息系统、县级单位中一般的信息统。

第二级信息系统：一般适用于县级其些单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。

第三级信息系统：一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；跨省或全 国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息系统以及这类系统在省、地市的分支系统；中央各部委、省（区、市）门户网站和重要网 站；跨省连接的网络系统等。

第四级信息系统：一般适用于国家重要领域、重要部门中的特别重要系统以及核心系统。例如电力、电信、广电、铁路、民航、银行、税务等重要、部门的生产、调度、指挥等涉及国家安全、国计民生的核心系统。

第五级信息系统：一般适用于国家重要领域、重要部门中的极端重要系统。

（二）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为业务信息安全等级。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等级。

确定信息系统安全保护等级的一般流程如下：确定作为定级对象的信息系统；确定业务信息安全受到破坏时所侵害的客体；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，根据业务信息的重要性和受到破坏后的危害性确定业务信息安全等级；确定系统服务安全受到破坏时所侵害的客体；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，根据系统服务的重要性和受到破坏后的危害性确定系统服务安全等级；由业务信息 安全等级和系统服务安全等级的较高者确定定级对象的安全保护等级。上述步骤如图 1-1 所示。

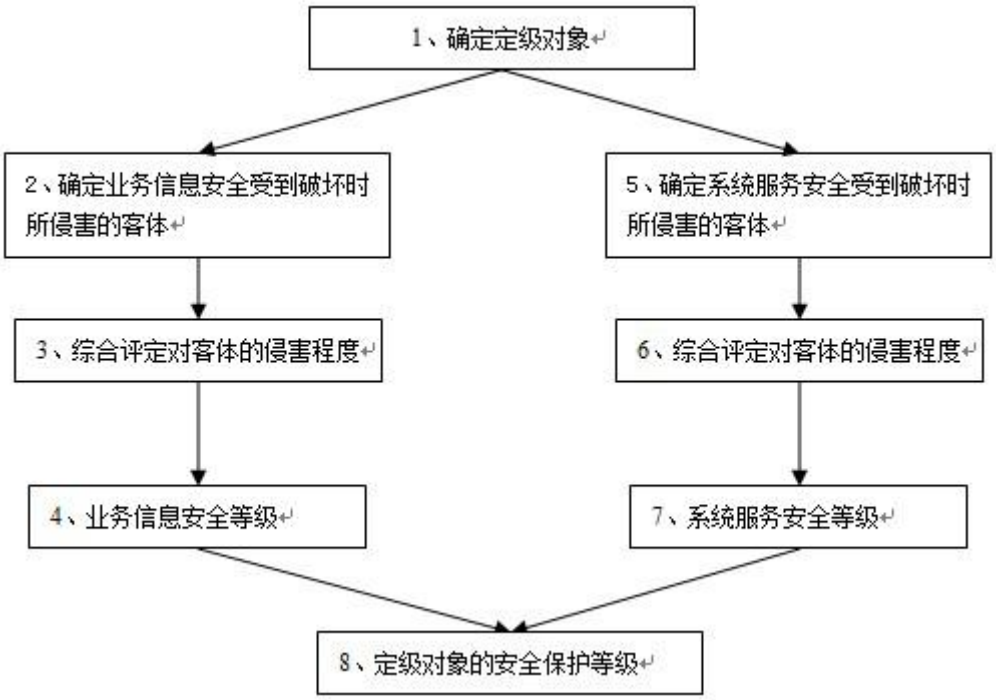

图 1-1 确定等级一般流程

1.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：影响国家机关社会管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，应首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公众利益，最后判断是否侵害公民、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。

2.确定对客体的侵害程度

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。

3.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断时，应参照以下不同的判别基准：

如果受侵害客体是公民、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断侵害程度的基准；

如果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断侵害程度的基准。

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。

特别严重损害：工作职能受到特别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、特别严重损害的具体定义。

4.确定信息系统安全保护等级

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 1-2 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 1-2 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	特别严重损害
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 1-3 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 1-3 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	特别严重损害
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。定级对象等级确定后，可参照附录 1 中的《信息系统安全保护等级定级报告》模版起草定级报告。

例如，“奥组委办公内网”承载奥组委内部的人事、财务等业务，仅在奥组委少数部门内应用，不传输秘密信息和敏感信息。其受到破坏后，会影响内部办公，会对社 会秩序、公共利益造成损害，定为二级；“奥组委办公外网”通过唯一出口与互联网相连，承载奥组委内部的电子邮件、物流、短信平台、场馆管理等业务，在奥组 委总部范围应用，其受到破坏后，会对社会秩序、公共利益造成损害，定为二级。“票务网站”负责提供票务申请、信息填写等业务，采集购票者信息和订票信息， 不与“票备管理系统”直接相连，其受到破坏后，会对社会秩序、公共利益造成损害，定为二级。“票务管理系统”存储处理通过各种方式申请、购买奥运票务的个 人数据，是“票备网站”的核心，其受到破坏后，会对社会秩序、公共利益造成严重损害，定为三级。“奥运官方网站”承担在互联网上对外宣传、报道奥运重大事 项，是北京奥运通过互联网对外宣传的门户，其服务器保障性要求很高，受到破坏后，会对社会秩序、公共利益造成严重损害，定为三级。“竞赛网”承担赛事安 排、计时、成绩统计等重大事项，其数据安全和服务保障性要求很高，受到破坏沿，会对社会秩序、公共利益造成严重损害，定为三级。

四、信息系统备案工作的内容和要求

（一）信息系统备案与受理

信息安全等级保护备案工作包括信息系统备案、受理、审核和备案信息管理等工作。信息系统运营使用单位和受理备案的公安机关应按照《信息安全等级保护备案实施细则》（公信安〔2007〕1360 号）的要求办理信息系统备案工作。

1.备案

第二级以上信息系统，在安全保护等级确定后 30 日内，由其运营、使用单位或者其主管部门（以下简称“备案单位”）到所在地设区的市级以上公安机关办理备案手续。办理备案手续时，应当首先到公安机关指定的网址下载并填写备案表，准备好备案文件，然后到指定的地点备案。

备案时应当提交《信息系统安全等级保护备案表》（以下简称《备案表》，参见附录 2）（一式两份）及其电子文档。第二级以上信息系统备案时需提交《备案表》中的表一、二、三；第三级以上信息系统还应当在系统整改、测评完成后 30 日内提交《备案表》表四及其有关资料。

隶属于中央的在京单位，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；其他信息系统向北京市公安局备案。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。各部委统一定级信息系统在各地的分支系统（包括终 端连接、安装上级系统运行的没有数据库的分系统），即使是上级主管部门定级的，也要到当地*备案。

2.受理备案

地市级以上公安机关公共信息网络安全监察部门受理本辖区内备案单位的备案。隶属于省级的备案单位，其跨地（市）联网运行的信息系统，由省级公安机关公共信息网络安全监察部门受理备案。

隶属于中央的在京单位，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，由公安部公共信息网络安全监察局受理备案，其他信息系统由北京市公安局公共信息网络安全监察部门受理备案。

隶属于中央的非在京单位的信息系统，由当地省级公安机关公共信息网络安全监察部门（或其指定的地市级公安机关公共信息网络安全监察部门）受理备案。

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在各地运行、应用的分支系统（包括由上级主管部门定级，在当地有应用的信息系统），由所在地地市级以上公安机关公共信息网络安全监察部门受理备案。

3.备案信息管理

公安部组织开发了重要信息系统安全监察管理系统，配发给各地，搭建一个部、省、市三级公安机关等级保护综合管理平台。该系统部、省两级公安机关部署，部、 省、市三级公安机关应用，为全国信息系统定级、备案和监督检查工作提供支持，为重要信息系统安全监察业务服务。各地公安机关要按照《关于部署开展等级保护 安全监察管理系统建设的通知》要求，组织本地开展系统建设，及时将定级备安和相关数据录入系统，利用该系统开展等级保护工作。

（二）公安机关受理备案要求

1.受理备案的公安机关公共信息网络安全监察部门应该设立专门的备案窗口，配备必要的设备和警力，专门负责受理备案工作，受理备案地点、时间、联系人和联系方式等应向社会公布。

2.接收备案材料后，公安机关应当对下列内容进行审核：备案材料填写是否完整，是否符合要求，其纸质材料和电子文档是否一致；信息系统所定安全保护等级是否准确。

3.公安机关收到备案单位提交的备案材料后，对属于本级公安机关受理范围且备案材料齐全的，应当向备案单位出具《信息系统安全等级保护备案材料接收回执》；备案 材料不齐全的，应当当场或者在五日内一次性告知其补正内容；对不属于本级公安机关受理范围的，应当书面告知备案单位到有管辖权的公安机关办理。

4.经审核符合等级保护要求的，公安机关应当自收到备安材料之日起的十个工作日内，将加盖本级公安机关印章（或等级保护专用章）的《备案表》一份反馈备案单位， 一份存档；对不符合等级保护要求的，公安机关公共信息网络安全监察部门应当在十个工作日内通知备安单位进行整改，并出具《信息系统安全等级保护备案审核结 果通知》。

5.《备案表》中表一、表二、表三内容经审核合格的，公安机关出具《信息系统安全等级保护备案证明》（以下简称《备案证明》）。《备案证明》由公安部统一监制。

6.受理备案的公安机关公共信息网络安全监察部门应当建立管理制度，对备案材料按照等级进行严格管理，严格遵守保密制度，未经批准不得对外提供查询。

（三）对定级不准以及不备案情况的处理

1.公安机关对定级不准的备案单位，在通知整改的同时，应当建议备案单位组织专家进行重新定级评审，并报上级主管部门审批。

2.备案单位仍然坚持原定等级的，公安机关可以受理其备案，但应当书面告知其承担由此引发的责任和后果，经上级公安机关同意后，同时通报备案单位上级主管部门。

3.对拒不备案的，公安机关应当根据《中华人民共和国计算机信息系统安全保护条例》等其他有关法律、法规规定，责令限期整改。逾期仍不备案的，予以警告，并向其上级主管部门通报。向中央和国家机关通报的，应当报经公安部同意。

（本文节选自公安部信息安全等级保护评估中心编写的《信息安全等级保护政策培训教程》）