



公
安
部

国家信息安全等级保护制度 的主要内容和要求

公安部 网络安全保卫局
郭启全



公
安
部

目 录

- 一、信息安全等级保护制度的主要内容
- 二、信息安全等级保护政策体系和标准体系
- 三、信息安全等级保护工作的具体内容和要求



一、等级保护制度的主要内容

（一）国家为什么要实施信息安全等级保护制度

1. 信息安全形势严峻

- ◆敌对势力的入侵、攻击、破坏
- ◆针对基础信息网络和重要信息系统的违法犯罪持续上升
- ◆基础信息网络和重要信息系统安全隐患严重



一、等级保护制度的主要内容

2. 是维护国家安全的需要

- ◆基础信息网络与重要信息系统已成为国家关键基础设施。
- ◆信息安全是国家安全的重要组成部分。
- ◆信息安全是非传统安全，信息安全本质是信息对抗、技术对抗。



公安
部

一、等级保护制度的主要内容

（二）国家对等级保护制度的要求

1. 《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）：“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”。



公安部

一、等级保护制度的主要内容

2. 《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）规定：要重点保护基础信息网络和关系国家安全的、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、等级保护制度的主要内容

（三）等级保护制度的地位和作用

- ◆ 是国家信息安全保障工作的基本制度、基本国策。
- ◆ 是开展信息安全工作的基本方法。
- ◆ 是促进信息化、维护国家信息安全的根本保障。



一、等级保护制度的主要内容

（四）实施等级保护制度的主要目的

- ◆明确重点、突出重点、保护重点。
- ◆有利于同步建设、协调发展。
- ◆优化信息安全资源的配置。
- ◆明确信息安全责任。
- ◆推动信息安全产业发展。

国家发展改革部门、财政部门、科技部门、公安机关对重要信息系统在政策上给予支持。



公安部

一、等级保护制度的主要内容

(五) 公安机关组织开展等级保护工作的依据

- 1、《警察法》规定：警察履行“监督管理计算机信息系统的安全保护工作”的职责。
- 2、国务院令第147号规定：“公安部主管全国计算机信息系统安全保护工作”，“等级保护的具体办法，由公安部会同有关部门制定”。
- 3、2008年国务院三定方案，公安部新增职能：“监督、检查、指导信息安全等级保护工作”。



公
安
部

全国公安机关网络安全保卫部门 机构和职责

机构：公安部：网络安全保卫局

各省：网络警察总队

地市：网络警察支队

区县：网络警察大队

部分职责：

制定信息安全政策

打击网络违法犯罪

互联网安全管理

重要信息系统安全监察

网络与信息安全信息通报



一、等级保护制度的主要内容

(六) 等级保护工作的主要内容

- ◆对信息系统分等级进行安全保护和监管。

五个规定动作：信息系统定级、备案、安全建设整改、等级测评、监督检查。

- ◆信息安全产品分等级使用管理。
- ◆信息安全事件分等级响应、处置。



一、等级保护制度的主要内容

(七) 相关部门的责任和义务

- ◆ **职能部门：**制定管理规范和技术标准，组织实施，开展监督、检查、指导。
- ◆ **行业主管部门：**督促、检查、指导本行业、本部门开展等级保护工作。
- ◆ **运营使用单位：**开展信息系统定级、备案、建设整改、等级测评、自查等工作，落实等级保护制度的各项要求。
- ◆ **安全服务机构：**开展技术支持、服务等工作，并接受监管部门的监督管理。



公安部

一、等级保护制度的主要内容

国家信息安全职能部门职责分工

- ◆ **公安机关：**牵头部门，监督、检查、指导信息安全等级保护工作。
- ◆ **国家保密部门：**负责等级保护工作中有关涉密工作的监督、检查、指导。并负责涉密及国家秘密信息系统分级保护。
- ◆ **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。
- ◆ **工业和信息化部门：**负责等级保护工作中部门间的协调。



一、等级保护制度的主要内容

（八）开展等级保护工作的基本要求

- ◆ 各单位、各部门，按照“准确定级、严格审批、及时备案、认真的整改、科学测评”的要求开展工作。
- ◆ 公安机关要及时开展监督检查，严格审查信息安全系统所定级、严格检查信息安全系统整改、测评等工作。
- ◆ 对故意将信息安全级别定低，逃避公安系统对安全保密、安全密码事故的监管，造成单位和人员责任的，要追究单位和相关人员的责任。



公
安
部

二、等级保护政策体系和标准体系

(一) 信息安全等级保护政策体系

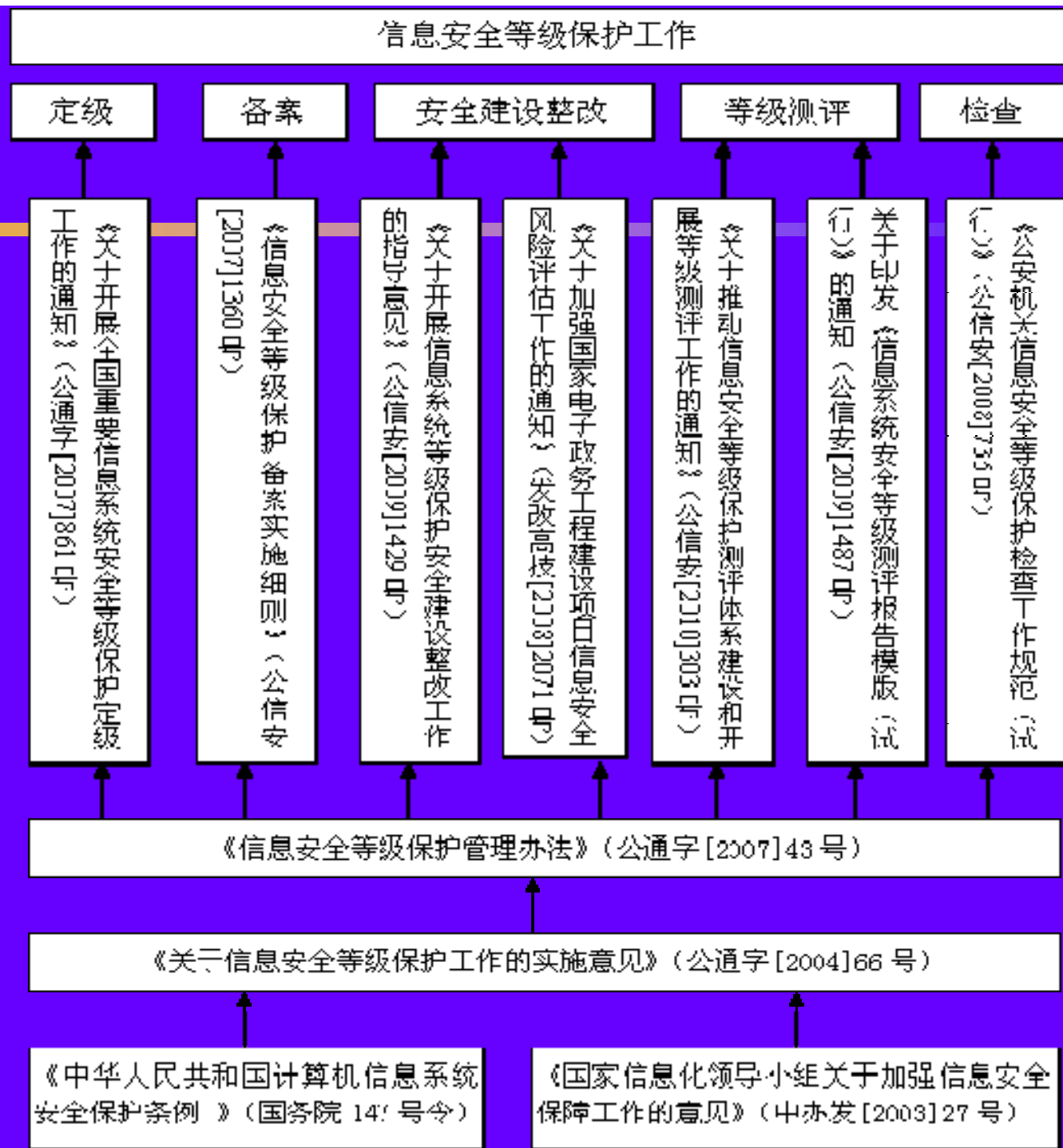
近几年，公安部根据国务院147号令的授权，会同国家保密局、国家密码管理局、发改委、原国务院信息办出台了一些文件，公安部对有些具体工作出台了一些指导意见和规范，构成了信息安全等级保护政策体系。

汇集成《信息安全等级保护政策汇编》供有关单位、部门使用。



公安部

在安全建设整改工作中的作用 等级保护有关政策





公
安
部

(一) 信息安全等级保护政策体系

- 1、《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）
- 2、《信息安全等级保护管理办法》公通字[2007]43号）
- 3、《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》（公通字[2007]861号）
- 4、《信息安全等级保护备案实施细则》（公信安[2007]1360号）
- 5、《关于开展信息系统等级保护安全建设整改工作的指导意见》公信安[2009]1429号）



公
安
部

（一）信息安全等级保护政策体系

- 6、《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071号）
- 7、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）。
- 8、《关于印发〈信息系统安全等级测评报告模版（试行）〉的通知》（公信安[2009]1487号）
- 9、《公安机关信息安全等级保护检查工作规范》（公信安[2008]736号）



公
安
部

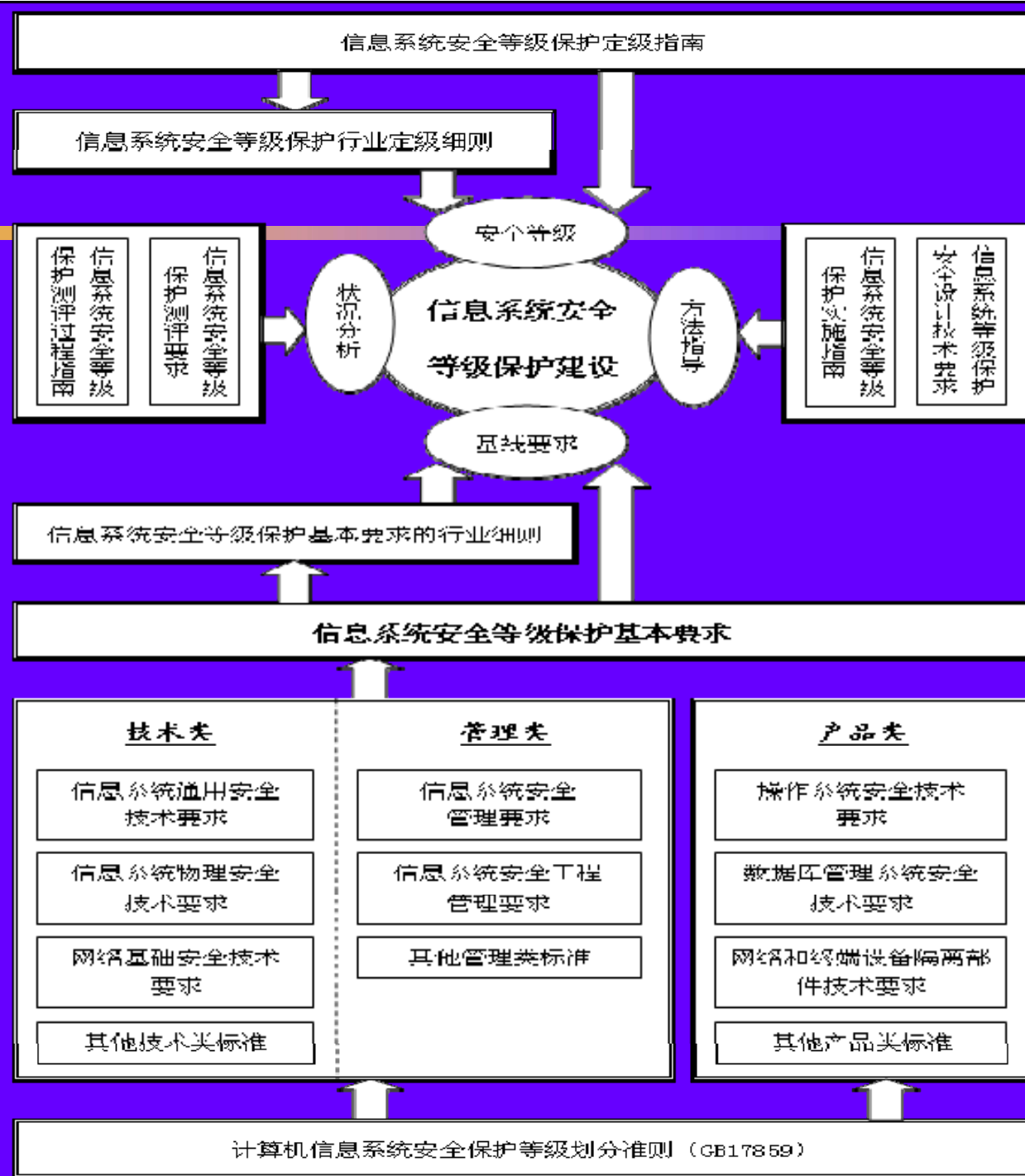
(二) 信息安全等级保护标准体系

多年来，在有关部门支持下，在国内有关专家、企业的共同努力下，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制订了信息安全等级保护工作需要的一系列标准，形成了比较完整的信息安全等级保护标准体系。汇集成《信息安全等级保护标准汇编》供有关单位、部门使用。



公安部

在安全建设整改工作中的作用 等级保护有关标准





公
安
部

(二) 信息安全等级保护标准体系

基础标准：

《计算机信息系统安全保护等级划分准则》。在此基础上制定出技术类、管理类、产品类标准。

安全要求：

《信息系统安全等级保护基本要求》
信息系统安全等级保护的行业规范



公安
部

(二) 信息安全等级保护标准体系

系统等级：

《信息系统安全等级保护定级指南》

信息系统安全等级保护行业定级细则

方法指导：

《信息系统安全等级保护实施指南》

《信息系统等级保护安全技术要求》

现状分析：

《信息系统安全等级保护测评要求》

《信息系统安全等级保护测评过程指南》



（二）信息安全等级保护标准体系

在应用有关标准中需注意的几个问题：

- 1、《基本要求》是阶段性目标，《信息系统等级保护安全技术要求》是实现该方法的目标和途径之一。
- 2、《基本要求》中不包含安全设计和工程实施等内容，因此可以参照《信息系统等级保护安全技术要求》等标准进行。
- 3、在进行安全建设整改时，应根据业务信息安全等级和系统服务安全等级确定《基本要求》中相应的安全保护要求。



公
安
部

(二) 信息安全等级保护标准体系

- 4、重点行业可以按照《基本要求》等国家标准，结合行业特点和特殊安全需求，在公安部等有关部门指导下，制定行业标准规范或细则。
- 5、《信息系统等级保护安全技术要求》提出“一个中心三维防护”（安全管理中心和计算环境安全、区域边界安全、通信网络安全）的安全保护设计技术要求。本标准应与其他标准配合使用。



公安
部

三、等级保护工作的具体内容和要求

(一) 信息安全等级保护定级工作

信息系统定级原则：“自主定级、专家评审、主管部门审批、公安机关审核”。具体可按照《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》（公通字[2007]861号）要求执行。

定级工作流程：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。



三、等级保护工作的具体内容和要求

1. 确定定级对象

- ◆起支撑、传输作用的信息网络（包括专网、内网、外网、网管系统）。
- ◆用于生产、调度、管理、指挥、作业、控制、办公等目的的各类业务系统。
- ◆各单位网站。



三、等级保护工作的具体内容和要求

2. 确定信息系统安全保护等级

《管理办法》规定的五个等级：

- ◆ 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。



公安部

三、等级保护工作的具体内容和要求

- ◆ 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特别严重损害，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，会对国家安全造成特别严重损害。



三、等级保护工作的具体内容和要求

实际操作中参考确定信息系统等级：

- ◆ **第一级信息系统：**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系统。
- ◆ **第二级信息系统：**适用于县级某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。



三、等级保护工作的具体内容和要求

- ◆ **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；跨省联接的网络系统等。



公安部

三、等级保护工作的具体内容和要求

- ◆ **第四级信息系统：**一般适用于国家重要领域、部门中涉及国家安全、电力生产控制网络、铁路客票系统、银行核心系统、国家业务系统、指挥系统、调度系统等。

3. 定级工作需注意的问题

- ◆ 同类信息系统的等级不能随着部、省、市行政级别的降低而降低。
- ◆ 新建系统在规划设计阶段应确定等级，按同照同步实施安全防护技术措施和管理措施。



公

安

部

三、等级保护工作的具体内容和要求

(二) 信息系统备案工作

备案工作包括：信息系统备案、受理、审核和备案信息管理。具体按照《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》要求开展。

1、备案

◆ 第二级以上信息系统，由信息系统运营使用单位到所在地设区的市级以上公安机关网络安全保卫部门办理备案手续，填写《信息系统安全等级保护备案表》。



公安部

三、等级保护工作的具体内容和要求

- ◆ 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备案；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，即使是上级主管部门定级的，也要到当地公安网络安全保卫部门备案。



公安部

三、等级保护工作的具体内容和要求

2. 受理备案与审核

公安机关受理备案，按照《信息安全等级保护备案实施细则》要求，对备案材料进行审核，定级准确、材料符合要求的颁发由公安部统一监制的备案证明。



三、等级保护工作的具体内容和要求

(三) 信息系统安全建设整改工作
充分认识工作的复杂性和艰巨性:

- ◆ 政策性和技术性很强。
- ◆ 涉及范围广。
- ◆ 信息系统安全加固改造，需要国家在经费上予以支持。
- ◆ 跨省全国联网的大系统结构复杂、运行实时保障性高、数据重要，加固改造周期长。



（三）信息系统安全建设整改工作

1、工作目标

- ◆ 利用三年时间。力争2012前完成。
- ◆ 开展三项重点工作：安全管理、技术措施建设和等级测评。
- ◆ 实现五方面目标：一是信息安全，二是信息保密，三是信息资源，四是信息应用，五是信息效益。



（三）信息系统安全建设整改工作

2、工作范围和工作特点

◆ 工作范围：

已备案的第二级（含）以上信息系统纳入安全建设整改的范围。

尚未开展定级备案的信息系统，要先定级备案，定级不准的要先纠正，再开展安全建设整改。

新建系统要同步开展安全建设工作。

◆ 工作特点：继承发展、引入标准、外部监督、政策牵引



（三）信息系统安全建设整改工作

3、工作方法

- ◆ 突出重要系统，兼顾二级。
- ◆ 试点示范，行业推广。
- ◆ 管理制度建设和技术措施建设同步或分步实施。
- ◆ 加固改造，缺什么补什么；也可以进行总体安全建设整改规划。
- ◆ 利用信息安全等级保护综合工作平台，使等级保护工作常态化。



（三）信息系统安全建设整改工作

4、工作内容

（1）等级保护安全管理制度建设

- 一是落实信息安全责任制。
- 二是落实人员安全管理制度。
- 三是落实系统建设管理制度。
- 四是落实系统运维管理制度。



公安部

(三) 信息系统安全建设整改工作

- ◆ 落实领导责任制。明确各级领导对信息系统安全工作的责任，实行“谁主管、谁负责”的原则，确保信息系统安全工作的落实。
- ◆ 落实岗位责任制。明确各级岗位工作人员的安全职责，实行“谁在岗、谁负责”的原则，确保信息系统安全工作的落实。
- ◆ 落实安全责任制。明确各级安全管理部门的安全职责，实行“谁主管、谁负责”的原则，确保信息系统安全工作的落实。
- ◆ 落实考核责任制。明确各级考核管理部门的考核职责，实行“谁考核、谁负责”的原则，确保信息系统安全工作的落实。
- ◆ 落实奖惩责任制。明确各级奖惩管理部门的奖惩职责，实行“谁奖惩、谁负责”的原则，确保信息系统安全工作的落实。



（三）信息系统安全建设整改工作

公安部

- ◆ 定码、工求。安全防等练，系
统密付确要境安码置演保
系、交明作环、代处展确
息用收，工房全意件开，
信使验度和机安恶事期段，
立购、制程立施、定手。
建采施理流建设全复并和实。
◆ 品实管作：备安恢案施落
度产程等工度设统与预措效
制、工务、制、系份急术有
理计、服法、理全、备应技的
管设发全方管安全、定理度
建设案开安作维质安护制管制
建文件、工运介络保，的理
统、软评、系统储网码度应管
系案、测容、系存、密制相维
实备用级内实、控、理取运
落级使等作落全监范管采统



公安
部

（三）信息系统安全建设整改工作

（2）等级保护安全技术措施建设

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，开展安全技术措施建设。

可以采取“一个中心三维防护”的防护策略，实现相应级别信息系统的安全保护技术要求。



公安 部

信息系统安全等级保护基本要求

安全管理建设整改

安全管理机构

- 岗位设置
- 人员配备
- 授权和审批
- 沟通和合作
- 审核和检查

人员安全管理

- 人员录用
- 人员离岗
- 人员考核
- 教育和培训
- 人员访问管理

安全管理制度

- 管理制度
- 制定和发布
- 评审和修订

系统运维管理

- 环境管理
- 资产管理
- 介质管理
- 设备管理
- 监控管理
- 安全管理中心
- 网络安全管理
- 系统安全管理
- 变更管理
- 备份恢复管理
- 事件处置
- 应急响应

系统建设管理

- 定级备案
- 安全方案设计
- 产品采购使用
- 自行软件开发
- 外包软件开发
- 工程实施
- 测试验收
- 系统交付
- 安全服务选择
- 等级测评

安全技术建设整改

物理安全

- 机房位置选择
- 防火防雷
- 防水防潮
- 防静电
- 物理访问控制
- 防盗窃防破坏
- 温湿度控制
- 电力供应
- 电磁防护

网络安全

- 区域划分
- 边界防护
- 访问控制
- 安全审计
- 入侵防范
- 病毒防护
- 通信保护

数据安全与备份恢复

- 数据保密性
- 数据完整性
- 备份与恢复

主机安全

- 身份鉴别
- 访问控制
- 安全审计
- 入侵防范
- 病毒防护
- 资源控制
- 安全标记
- 剩余信息保护

应用安全

- 身份鉴别
- 访问控制
- 安全审计
- 通信完整性
- 通信保密性
- 软件容错
- 资源控制
- 安全标记
- 剩余信息保护
- 抗抵赖



公安
部

(三) 信息系统安全建设整改工作

信息系统安全建设整改方案主要内容:

- ◆ 项目背景
- ◆ 政策和技术标准依据
- ◆ 安全需求分析
- ◆ 安全建设整改技术方案设计
- ◆ 安全建设整改管理体系设计
- ◆ 信息系统安全产品选型及技术指标
- ◆ 安全建设整改后信息系统残余风险分析
- ◆ 安全建设整改项目实施计划
- ◆ 项目预算



（三）信息系统安全建设整改工作

5、工作流程

第一步：制定安全建设整改工作计划，对安全建设整改工作进进行总体部署。

第二步：开展信息系统安全现状分析，从管理和技术两方面确定安全建设整改需求。

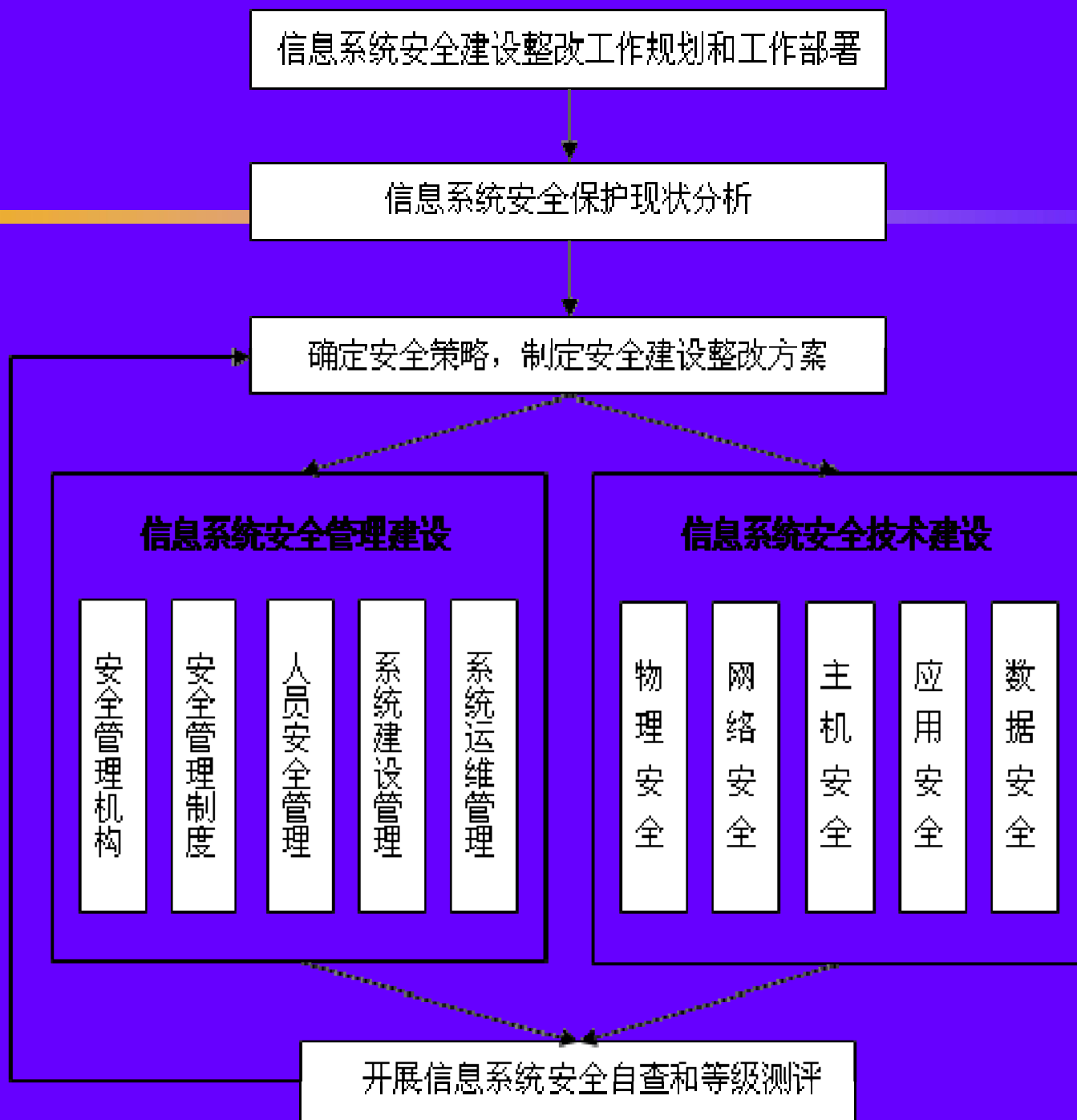
第三步：确定安全保护策略，制定信息系统安全建设整改方案。

第四步：开展信息系统安全建设整改工作，建立并落实安全管理制度，落实安全责任，建设安全设施，落实安全措施。

第五步：开展安全自查和等级测评，及时发现并进一步整改。



公安部





（三）信息系统安全建设整改工作

6、信息系统应达到的保护能力目标

第二级信息系统：经过安全建设整改工作，信息系统具有抵御小规模、较弱的恶意攻击的能力，抵抗一般的自然灾害的能力，防范一般性计算机病毒和恶意代码危害的能力；具有检测常见的攻击行为，并对安全事件进行记录的能力；系统遭到损害后，具有恢复系统正常运行状态的能力。



公安部

(三) 信息系统安全建设整改工作

第三级信息系统：经过安全建设整改工作，御严密、行在运系统的作，信大重意记响系行系统能息规的代录应系统状，资力。系统模、然危侵置到的能、在较灾害行，损能立用统强害的为并害力即户、一恶的能的能后，恢、的意能力能够，对复安安全攻击，具；踪有服常机保护的防有具安能务运制保护能范检有全够保行等策略，算、安任快性态；集具抗病现事能复求具中下抵机发全的恢要；集



公安部

(三) 信息系统安全建设整改工作

第四级信息系统：经过安全建设整改具力，病现事任快性态；集整下能机发全责较障状行策略的算、安全能够保行进策击计测对安能务运等全护攻范检有踪有服常制安保模防有具追具于正机安大力；力能够，对复安全规，具；够，对复安的能力能并害力速；恢安的能，损能迅户、组织的能的，损能迅户、统组害的为置到的能用在有灾害行处遭态应、系统力然危侵应系统状，源、系统势自码入响系行系统资力。信息对的代录速在运系统能信敌重意记快；常的系的作，御严恶、行力正高对管工有抵抗和警进能复求有控有抵毒报件的恢要具中



三、等级保护工作的具体内容和要求

(四) 信息安全等级保护测评工作

等级测评是测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密的信息系统安全等级保护状况进行检测评估的活动。是信息安全等级保护工作的重要环节。

公安机关按照《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）要求，开展测评机构和测评人员的管理工作，保证等级测评的客观、公正和安全。



三、等级保护工作的具体内容和要求

1、测评机构和测评人员的管理

(1) 职责分工

- ◆ 国家信息安全等级保护工作协调小组办公室（以下简称“部保办”）负责测评机构的申请受理、审核推荐和监督检查等工作。
- ◆ 各省级等保办负责等级测评机构的申请受理、审核推荐和监督检查等工作。
- ◆ 公安部信息安全等级保护评估中心（以下简称“信评中心”）负责测评机构的能力



三、等级保护工作的具体内容和要求

(2) 测评机构申请流程

- ◆ 申请：申请单位向省级以上等保办书面申请，提交《信息安全等级保护测评机构申请表》。
- ◆ 受理、初审：等保办受理申请，并对申请材料进行初审。
- ◆ 能力评估：公安部信息安全等级保护评估中心对申请单位进行能力评估，对测评师进行培训、考试、发证。



三、等级保护工作的具体内容和要求

- ◆ 专家审核：等保办组织专家对测评能力评估合格的申请单位进行审核。
- ◆ 推荐：等保办向通过评审的申请单位颁发信息安全等级保护测评机构推荐证书。
- ◆ 公布。省级等保办向社会公布测评机构推荐目录并报国家等保办，国家等保办汇总公布《全国信息安全等级保护测评机构推荐目录》。



三、等级保护工作的具体内容和要求

(3) 监督管理

- ◆ 日常监督：测评报告、测评过程、测评服务费用。
- ◆ 变更处理：机构名称、法人、测评师等变动的，在30日内到等保办办理变更。
- ◆ 违规处置：限期整改、警告、取消证书。
- ◆ 年度检查：检查时间、内容、方式。



公安
部

三、等级保护工作的具体内容和要求

测评机构不得从事下列活动：

- （一）影响被测评信息系统正常运行，危害被测评信息系统安全；
- （二）泄露知悉的被测评单位及被测评信息系统的国家秘密和工作秘密；
- （三）故意隐瞒测评过程中发现的安全问题，或者在测评过程中弄虚作假，未如实出具等级测评报告；
- （四）未按规定格式出具等级测评报告；



公安
部

三、等级保护工作的具体内容和要求

- (五) 非授权占有、使用等级测评相关资料及数据文件;
- (六) 分包或转包等级测评项目;
- (七) 信息安全产品开发、销售和信息系统安全集成;
- (八) 限定被测评单位购买、使用其指定的信息安全产品;
- (九) 其他危害国家安全、社会秩序、公共利益以及被测单位利益的活动。



三、等级保护工作的具体内容和要求

2、等级测评工作的开展

- ◆ 测评目的：一是掌握信息系统安全状况、排查系统安全隐患和薄弱环节、明确信息系统安全建设整改需求；二是能够衡量出信息系统安全保护措施是否符合等级保护基本要求，是否具备了相应等级的安全保护能力。



公
安
部

三、等级保护工作的具体内容和要求

- ◆ 测评时机：建设整改前：等级测评，现状分析；建设整改后：等级测评，检验整改效果。
- ◆ 测评频率：第三级以上定期；第二级参照。
- ◆ 测评费用：参照国家信息化项目人工计费标准或根据被测设备数量与测评项预算测评费用。



三、等级保护工作的具体内容和要求

◆ 测评工作要求：

测评工作应按照“流程规范、方法科学、结论公正”的要求进行。

被测单位要监督管理测评机构和测评人员的测评活动；与测评机构签订工作协议和保密协议；查验相关材料；落实测评过程监管措施。

测评报告备案：备案单位每年应将等级测评报告向受理备案的公安机关备案



三、等级保护工作的具体内容和要求

3、测评业务范围

- ◆ 职能部门测评机构在全国范围内开展测评业务，到地方时，应当事先告知属地省级等保办。
- ◆ 行业测评机构原则上在本行业内开展测评，到地方时应与属地省系的保测评任务协调。可以承担其他行业信息系统的测评任务。
- ◆ 地方测评机构原则上在本地开展测评，也可以到异地开展测评，但事先须与当地的等保办协调。可以承担各部委信息系统的测评任务。
- ◆ 特殊情况由公安机关进行协调。



三、等级保护工作的具体内容和要求

(五) 安全自查和监督检查

备案单位、行业主管部门、公安机关要分别建立并落实监督检查机制，定期开展监督检查。

1、备案单位的定期自查

- ◆ 定期开展自查，掌握信息系统安全状况、安全管理制度及技术保护措施落实情况等。
- ◆ 配合公安机关的监督检查工作，如实提供有关资料及文件。当重要信息系统发生事件、案件时，备案单位应当及时向受理备案的公安机关报告。



三、等级保护工作的具体内容和要求

2、行业主管部门的督导检查

- ◆ 行业主管部门要建立督导检查制度，组织制定本行业、本部门的信息安全等级保护检查工作规范。
- ◆ 定期组织对本行业、本部门等级保护工作开展情况进行检查，督促落实信息安全等级保护制度，达到重点督促，以点带面的目的。



公安部

三、等级保护工作的具体内容和要求

3、公安机关的监督检查

- ◆ “谁受理备案、谁负责检查”。依据《公安机关信息安全等级保护检查工作规范（试行）》开展监督检查。
- ◆ 会同主管部门共同开展，建立监督检查配合机制。
- ◆ 对重要信息系统发生的事件、案件及时进行调查和立案侦查，并指导开展应急处置工作。



三、等级保护工作的具体内容和要求

(六) 信息安全产品的选择使用

1、信息安全产品在市场上销售，必须通过公安部信息安全产品检测中心检测，并获得公安部颁发的销售许可证。

2、公安部发布了《关于调整更新计算机信息系统安全专用产品检测执行标准规范的公告》（公信安[2009]1157号），对已有分级标准的29类信息安全产品开展分级检测工作。对于检测并审核通过的产品，产品销售许可证书标注产品分级信息，便于用户选择使用。



三、等级保护工作的具体内容和要求

3、《管理办法》规定，第三级以上信息系统应当选择使用我国自主研发的信息安全产品。信息安全产品是信息安全的基础，尤其是进入到重要系统中的信息安全产品将直接影响信息系统的的核心安全。因此，应在满足使用要求的前提下，优先选择国产产品。



公
安
部

谢谢!