国家信息安全等级保护法律政策

公安部　网络安全保卫局
郭启全

公安部

公安机关网络安全保卫部门机构和职责

公安部

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

职责：制定网络安全政策
打击网络违法犯罪
互联网安全管理
重要信息系统安全监管
网络安全通报预警

目 录

公安部

一、我国网络安全面临的新形势
二、我国关键信息基础设施安全保障方面存在的突出问题
三、IT企业在国家网络安全保障工作中如何充分发挥技术支撑作用
四、国家有关信息安全等级保护的法律政策要求
五、信息安全等级保护工作主要内容

一、我国网络安全面临的新形势

公安部

1、某些国家对我网络安全构成最大威胁

- 加快战略布局，强夺网络空间制高点
- 强力推进网军建设，加快网络战备战，对我构成战略威慑
- 扩大网上统一战线，抢占网络空间国际规则制定主导权
- 使用各种方法，利用网络对我实施控制、攻击和窃密
- 日本、菲律宾等领土领海争端国对我网络安全构成严重威胁

公安部

2、敌对势力和黑客组织的严重威胁

- 近年来敌对势力、敌对组织利用互联网对我政府网站、基础信息网络、重要信息系统进行入侵攻击、控制和窃密。
- “反共黑客联盟”攻击我政府网站，篡改网页张贴反动标语。
- 全球最大的黑客组织“匿名者”在全球拥有60万成员，该组织号召力极强，具备实施大规模网络攻击的能力，多次对我政府网站发动攻击。

公安部

3、互联网快速发展带来的严重挑战

- 网络社会的快速发展深刻影响着现实社会的政治、经济、文化等诸多方面。
- 互联网已成为敌对势力、敌对分子图谋颠覆我政权的主要抓手。
- 网络恐怖成为国家安全新的重大威胁。
- 电子商务安全影响国家经济安全和社会稳定。

公安部

原美国国务卿舒尔茨、奥尔布赖特妄言，有了互联网，就有了对付中国的办法。

公安部

4、关键信息基础设施安全隐患严重

- 境外一些企业的产品和服务，已深度渗透至我国电信、金融、能源等关键信息基础设施。
- 我重要行业部门选用国外操作系统、数据库、服务器、核心路由器等关键信息产品，这些国外产品很多都被情报机构预置了后门或植入了木马，这些产品中的后门、漏洞客观上成为了窃密渠道和网络攻击的通道。

公安部

5、新技术新应用的加快发展给网络安全带来了更大的风险和隐患

- 下一代互联网、物联网、云计算、大数据、移动互联网等加快应用，实现“智能电网”、“智能油田”和“智慧城市”
- 云计算的虚拟化、集约化的安全，物联网感知层、传输层的安全，智能位置服务的位置隐私安全，大数据的海量数据安全，移动互联网的智能端安全，成为了网络安全新的挑战。

公安部

6、网络违法犯罪活动呈快速增长

- 利用和针对互联网实施网络窃密、网络赌博、网络诈骗、网上盗窃等违法犯罪活动，日益猖獗。
- 不法分子利用各种手段窃取、贩卖公民个人信息，从事各种违法犯罪活动，涉及金融、电信、交通、教育、医疗、国土、工商、物业、保险、快递等行业。
- 网上制造传播谣言，进行有组织敲诈，严重扰乱社会秩序。

二、我国关键信息基础设施安全保障方面存在的突出问题

公安部

一是重要行业部门对网络安全认识不清，安全意识差，重视不够。缺少全局性的政策文件、标准，缺乏对整个工作的指导

二是缺乏顶层设计和规划，缺乏统一领导。安全保护策略不科学

三是管理体制机制不顺。管理制度不健全，责任部门、责任人不落实，安全责任不落实，职责不清，分工不明

四是缺乏在机构设置、人员配备、机制、能力等方面的整体考虑和统筹

公安部

五是主动发现能力差。缺少安全技术措施和管理措施，发现入侵攻击、窃密和网络系统安全隐患、问题能力差

六是主动防护能力差。防攻击、防窃密、防篡改等技术措施和管理措施不落实。

七是应急处置能力差。缺少信息系统应急处置预案。缺乏组织应急演练，预案不起任何作用。

八是创新不够。在策略、技术、产品等方面的改革创新需要加强。

公安部

九是重点工作不落实。等级保护、安全监测、通报预警、应急演练、灾备、安全检查等工作不深入。工作机制、标准、机构、人员、经费等基础保障能力差

十是没有认真落实网络安全与信息化建设“同步规划、同步设计、同步实施”的三同步要求。对信息系统缺乏全生命周期管理。在系统规划、建设、运维等阶段“重开发、重应用、轻安全”。隐患排查不强，日志存储、分析能力不强。

三、IT企业在国家网络安全保障工作中如何发挥好技术支撑作用

公安部

一是充分了解和掌握习总书记和党中央对网络安全工作的重大决策部署

- 2013年12月30日中央成立网络安全和信息化领导小组。
- 2014年2月27日召开第一次会议。习近平总书记指出：“没有网络安全，就没有国家安全；没有信息化，就没有现代化”，“网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”。

公安部

- 网络安全关系到七个重点：意识形态安全、技术安全、数据安全、应用安全、边防安全、资本安全、渠道安全。
- 习近平总书记提出建设网络强国战略目标：技术要强、内容要强、基础要强、人才要强、国际话语权要强。
- 2015年1月28日习近平总书记支持召开第二次领导小组会议。指出：依靠群众力量坚定不移。牢牢把握核心技术这个战略“撒手锏”。

公安部

二是充分了解和掌握国家和网络安全职能部门的政策

- 《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）。
- 全国人大《关于加强网络信息保护的决定》
- 《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》国发[2012]23号

公安部

- 《国务院关于推进物联网有序健康发展的指导意见》国发[2013]7号
- 公安部、发改委和财政部联合印发的《关于加强国家级重要信息系统安全保障工作有关事项的通知》（公信安[2014]2182号）
- 中央综治办印发《2014年综治工作（平安建设）考核评价实施细则》（中综办[2014]16号），将“信息安全保障工作”纳入对政府的考核。

公安部

- 2014年8月国家发改委等八部委联合印发了《关于促进智慧城市健康发展的指导意见》（发改高技[2014]1770号）文件
- 2014年11月国家发改委印发了《促进智慧城市健康发展部际协调工作制度及2014-2015工作方案》（发改办高技[2014]2652号）文件。在全国“智慧城市”建设26个部委参加的协调机制中，明确规定由公安部开展“智慧城市”网络安全建设、管理和评价工作。

公安部

三是为重要行业部门落实重要安全管理和技术措施提供技术支撑

- 变产品提供商为综合服务提供商。开展安全咨询、规划设计，制定安全建设方案，安全建设整改实施，安全运维，安全监理，安全监测，应急处置和安全检查技术支持。
- 落实网络安全与信息化建设三同步要求。“同步规划、同步设计、同步实施”。
- 开展云计算、物联网、工控系统、移动互联网的安全保护方法研究，标准研究。

公安部

四是加强在策略、技术、产品等方面的改革和创新

- 采取“人防、物防、技防、制防”管理策略，和“安全分区、网络专用、横向隔离、纵向认证”等保护策略，提高网络安全防护的科学性和综合防护能力。
- 按照“攻不进、拿不走、看不懂”的策略，落实一些“管用”措施：
  - 统一防护、整体防护。
  - 建设监测系统，实时监控。

公安部

统一防护、整体防护。

边界控制强逻辑隔离

利用密码技术、设备对数据、传输加密。最后一道防线。

操作系统加固。

渗透性攻击测试，检验系统防攻击能力。

定期修改口令，解决系统默认口令、弱口令、通用口令问题。定期查找并修补漏洞

公安部

虚拟机、沙箱技术。

终端主动防御。

黑、白名单技术（私有云服务）

产品联动（云端、边界、终端）。

大数据技术（关联分析、日志存储与分析，可发现、可追溯）。

审计措施、设备要采用（可追踪追溯）

四、国家有关信息安全等级保护的法律政策要求

公安部

1. 《中华人民共和国人民警察法》规定：人民警察履行“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，赋予公安部“监督、检查、指导信息安全等级保护工作”法定职责。

公安部

4.《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：实行信息安全等级保护。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 。

5.《国务院关于推进信息化发展和切实保障信息安全的若干意见》（国发[2012]23号）：“落实信息安全等级保护制度，开展相应等级的安全建设和管理，做好信息系统定级备案、整改和监督检查。”

公安部

6. 国家发改委、公安部、财政部、国家保密局、国家电子政务内网建设和管理协调小组办公室联合印发了《关于进一步加强国家电子政务网络建设和应用工作的通知》（发改高技[2012]1986号）

7. 公安部、发改委和财政部联合印发的《关于加强国家级重要信息系统安全保障工作有关事项的通知》（公信安[2014]2182号）要求，加强对47个行业、276家单位、500个涉及国计民生的国家级重要信息系统的安全监管和保障。

公安部

8.2014年12月，中办国办《关于加强社会治安防控体系建设的意见》要求：“完善国家网络安全监测预警和通报处置工作机制，推进完善信息安全等级保护制度”。

9.2014年12月中央批准实施的《关于全面深化公安改革若干重大问题的框架意见》指出，“推进健全信息安全等级保护制度，完善网络安全风险监测预警、通报处置机制”。

10.《中央网络安全和信息化领导小组2015年工作要点》中，要求“落实国家信息安全等级保护制度”。

五、信息安全等级保护工作主要内容

（一）信息安全等级保护工作的内涵

- 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、分等级监管。
- 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。
- 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。

公安部

公安部

- **定级：**将信息系统（包括网络）按照重要性和遭受损坏后的危害性分成五个安全保护等级；
- **备案：**等级确定后，第二级（含）以上信息系统到公安机关备案，公安机关审核后颁发备案证明；
- **测评：**备案单位选择符合国家规定条件的测评机构开展等级测评；
- **建设整改：**备案单位根据信息系统安全等级，按照国家政策、标准开展安全建设整改；
- **检查：**公安机关定期开展监督、检查、指导。

公安部

（二）职责分工

- 公安机关牵头，制定政策标准，并进行监督、检查、指导
- 国家保密部门、密码管理部门负责有关保密工作和密码工作的监督、检查、指导
- 网信办负责等级保护工作中部门间的协调

其中，涉及国家秘密信息系统由国家保密部门负责；非涉及国家秘密信息系统由公安机关负责

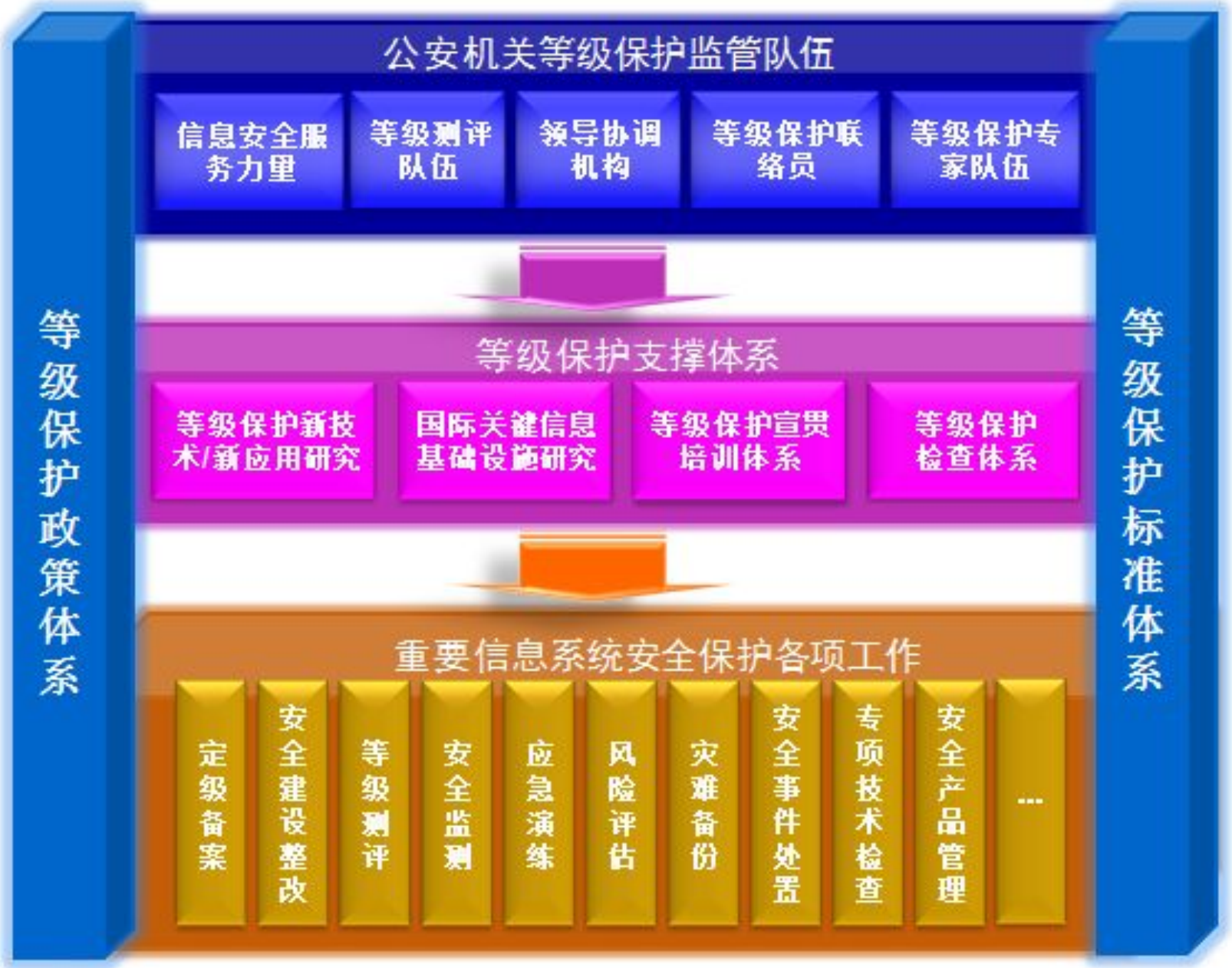
公安部

- 相关部门责任和义务

- **监管部门：**制定管理规范和技术标准，组织实施，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。

信息安全等级保护工作体系框架图

公安部



公安部

（三）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、认真整改、科学测评”的要求开展等级保护的定级、备案、整改、测评等工作。
- 公安机关要及时开展监督检查，严格审查信息系统所定级别，严格检查信息系统开展备案、整改、测评等工作。
- 对故意将信息系统安全级别定低，逃避公安、保密、密码部门监管，造成信息系统出现重大安全事故的，要追究单位和人员的责任。

公安部

（四）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

等级保护工作配套政策体系

信息安全等级保护工作

定级 | 备案 | 安全建设整改 | 等级测评 | 检查

《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）

《信息安全等级保护备案实施细则》（公信安[2007]1360 号）

《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）

《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

《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

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）

《关于开展信息安全等级保护专项监督检查工作》的通知（公信安[2010]1175 号）

《公安机关信息安全等级保护检查工作规范（试行）》（公信安[2008]736 号）

《信息安全等级保护管理办法》（公通字[2007]43 号）

《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）

《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）

公安部

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

6.《关于做好信息安全等级保护测评机构审核推荐工作的通知》（公信安[2010]559号）

7.《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）

8.《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）。

9.《关于加强信息安全等级保护测评重点工作的通知》（公信安[2014]2084号）

公安部

10.《公安机关信息安全等级保护检查工作规范》（公信安[2008]736号 ）

11.《关于开展信息安全等级保护专项监督检查工作的通知》（公信安[2010]1175号）

12.《关于进一步推进中央企业信息安全等级保护工作的通知》（公通字[2010]70号）

13.《关于加强政府网站安全监管工作的指导意见》（公信安〔2014〕353号）

14.《关于组织开展信息安全保障工作全国综治考核评价的通知》公信安[2014]2759号

公安部

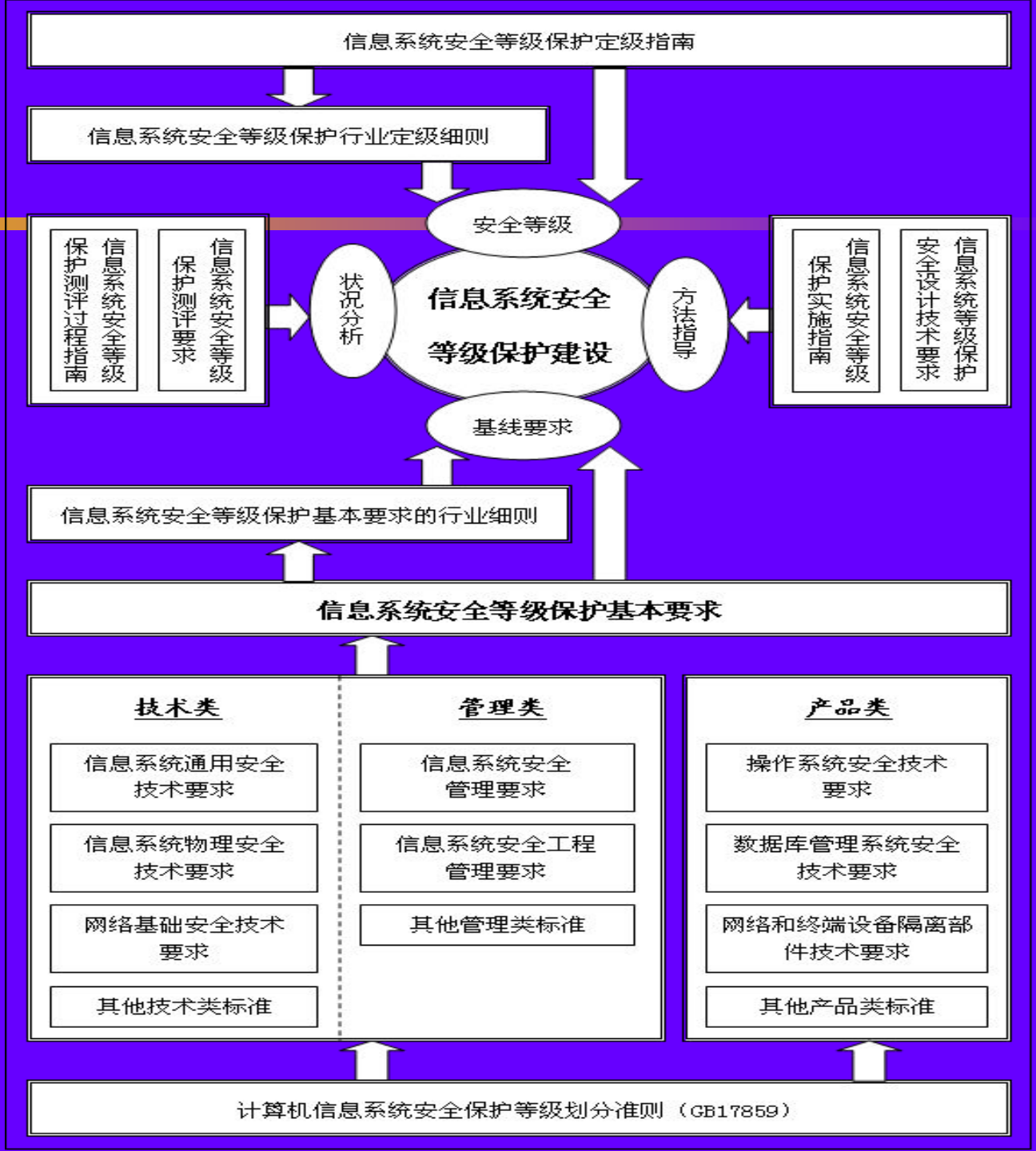
（五）信息安全等级保护标准体系

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

- **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

- **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设计技术要求》
- **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》

公安部

（六）信息安全等级保护工作具体内容和要求

1、信息安全等级保护定级工作

（1）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。

（2）定级工作流程：摸底调查、确定定级对象、对信息系统进行重要性分析、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。

公安部

（3）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 。
- 各类网站。

（4）确定信息系统安全保护等级：

根据信息系统重要性分析结论，按照《管理办法》要求确定等级。

公安部

信息系统五个安全保护等级：

- 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。
- 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。

公安部

- 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。

实际定级中可参考下面操作：

- **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。

公安部

- **第二级信息系统**：适用于县级单位中的信息系统；地市以上国家机关、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**：适用于地市以上机关、企事业单位内部重要信息系统，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；跨省或全国联网的用于生产、调度、管理、指挥、作业、控制等方面的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

- **第四级信息系统：**一般适用于国家重要领域、部门中涉及国计民生、国家利益、国家安全，影响社会稳定的核心系统。例如电力生产控制系统、银行核心业务系统、电信骨干传输网、铁路客票系统、列车指挥调度系统等。

定级工作需注意的问题：

- 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。
- 新建系统在规划设计阶段应确定等级，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。

公安部

（5）组织专家评审

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，可以聘请公安部和各地公安机关组织成立的专家组进行评审，并出具专家评审意见。

（6）主管部门审批

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。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，确保定级的一致性。

公安部

2、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）备案流程

- 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

- 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

（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。发现定级不准的，通知备案单位重新审核确定。

（3）备案管理

将备案信息系统录入重要信息系统安全管理系统进行管理。

公安部

3、信息安全等级保护测评工作

（1）测评工作性质：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。

（2）测评的目的：查找重要信息系统安全隐患、漏洞、薄弱环节和安全问题，对照国家标准查找信息系统安全保护情况与基本要求的差距，为开展安全建设提供依据。

公安部

（3）等级测评工作的组织：备案单位选择《全国信息安全等级保护测评机构推荐目录》 中推荐的测评机构，对第三级以上信息系统每年开展一次等级测评。

（4）测评机构的选择：凡列入《全国信息安全等级保护测评机构推荐目录》中测评机构，开展测评活动不受行业、地区限制，各地、各行业不得以各种理由排斥。

（5）关于测评费用问题。由于测评工作属于信息化服务和信息安全服务，所以，备案单位可按照有关部门出台的服务收费标准合理支付测评费用。

公安部

4、信息系统安全建设整改工作

（1）工作目标

- 开展安全管理制度建设和技术措施建设。
- 实现五方面目标：一是信息系统安全管理水平明显提高，二是信息系统安全防范能力明显增强，三是信息系统安全隐患和安全事故明显减少，四是有效保障信息化健康发展，五是有效维护国家安全、社会秩序和公共利益。

公安部

（2）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。

（3）工作方法

- 管理制度建设和技术措施建设并重。
- 安全建设整改总体规划、实施。加固改造，缺什么补什么。

公安部

（4）工作内容

以《信息系统安全等级保护基本要求》为目标，从管理和技术两方面进行安全建设整改。

- 等级保护安全管理建设整改

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

- 等级保护安全技术措施建设整改

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，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。

可以采取“一个中心三维防护（即一个安全管理中心和计算环境安全、区域边界安全和通信网络安全）” 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

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

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

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

数据安全与备份恢复
- 数据保密性
- 数据完整性
- 备份与恢复

公安部

（5）安全建设方案主要内容

- 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

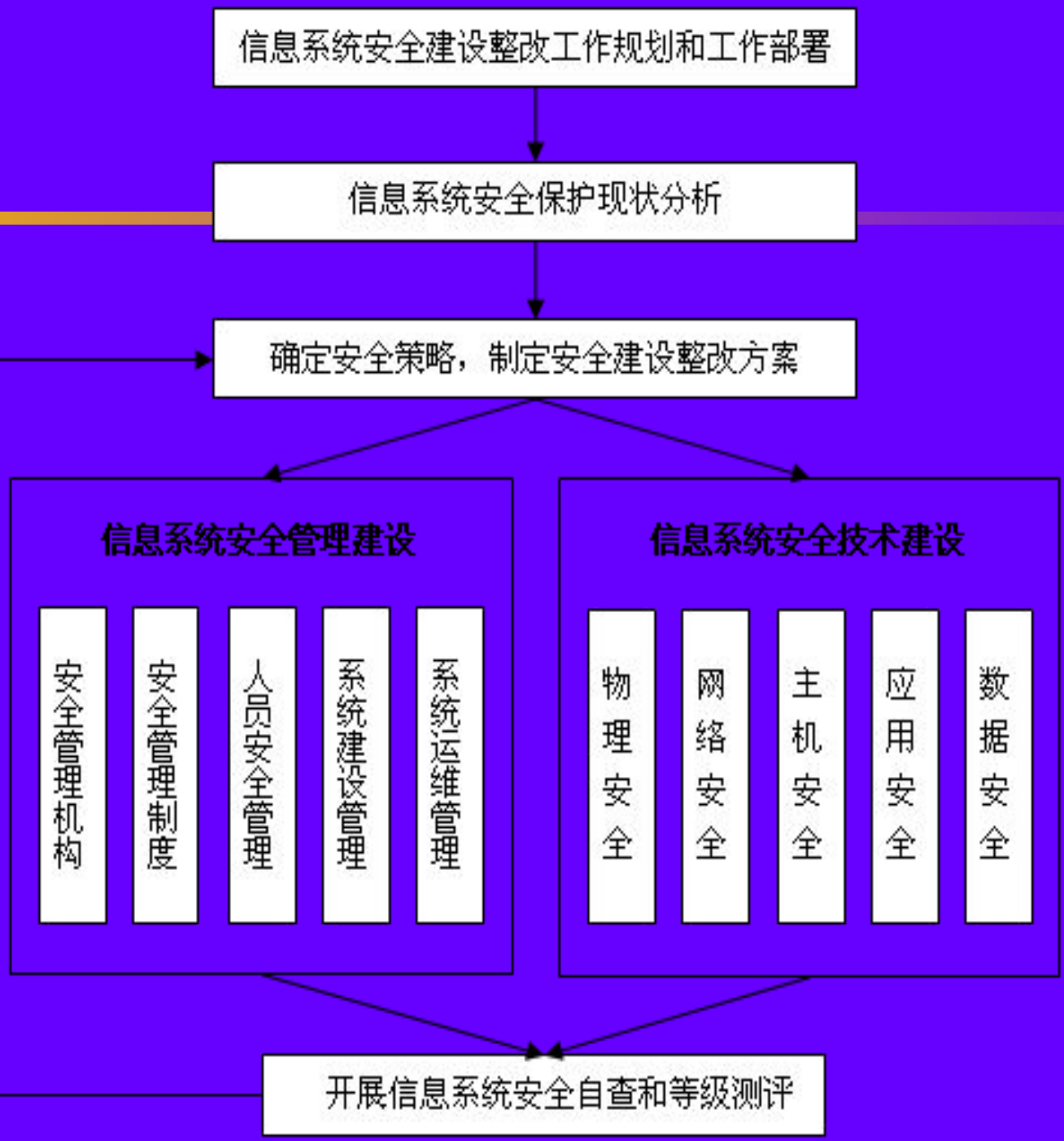
公安部

（6）工作流程

- 制定安全建设整改工作规划，对安全建设整改工作进行总体部署。
- 开展等级测评，对信息系统进行安全现状分析，从管理和技术两方面确定安全建设整改需求。
- 确定安全保护策略，制定信息系统安全建设整改方案。
- 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，落实安全责任制，建设安全设施，落实安全措施。
- 开展安全自查和等级测评，及时发现问题并进一步整改。

公安部

工作流程


信息系统安全建设整改工作规划和工作部署
信息系统安全保护现状分析
确定安全策略，制定安全建设整改方案
信息系统安全管理建设
安全管理机构
安全管理制度
人员安全管理
系统建设管理
系统运维管理
信息系统安全技术建设
物理安全
网络安全
主机安全
应用安全
数据安全
开展信息系统安全自查和等级测评

公安部

（7）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、较弱强度恶意攻击的能力，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

第三级信息系统：经过安全建设整改工作，信息系统在统一的安全保护策略下具有抵御大规模、较强恶意攻击的能力，抵抗较为严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能立即恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

公安部

第四级信息系统：经过安全建设整改工作，信息系统在统一的安全保护策略下具有抵御敌对势力有组织的大规模攻击的能力，抵抗严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行快速响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能迅速恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

公安部

5、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的落实情况等。
- 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。

公安部

（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

（3）公安机关的监督检查

- 依据《关于开展信息安全等级保护专项监督检查工作的通知》（公信安[2010]1175）和《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。

公安部

- 检查内容：
- 等级保护工作部署和组织实施情况
- 信息系统安全等级保护定级备案情况
- 信息安全设施建设情况和信息安全整改情况
- 信息安全管理制度建立和落实情况
- 信息安全产品选择和使用情况
- 聘请测评机构开展技术测评工作情况
- 定期自查情况

公安部

谢 谢！