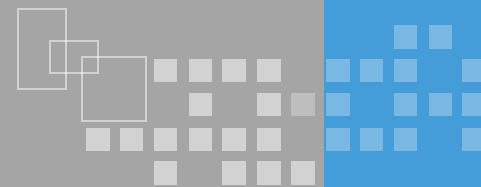




网络安全监管

版本：4.2

齐文振 河南信安世纪



网络安全监管

网络安全法律体系建设

国家网络安全政策

网络安全道德准则

信息安全标准

知识域

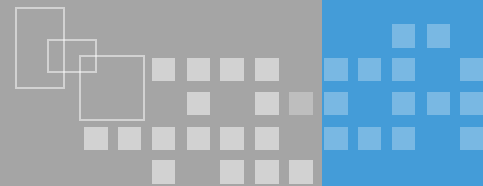
知识子域

❖ 计算机犯罪

- 了解计算机犯罪的概念、特征及计算机犯罪的发展趋势。

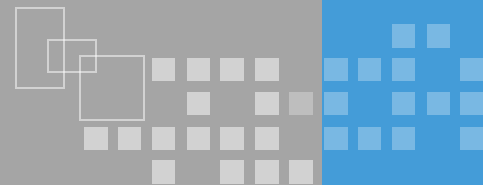
❖ 我国立法体系

- 了解我国多级立法机制及相关职能；
- 了解立法分类（法律、行政法规及地方性法规）等概念。

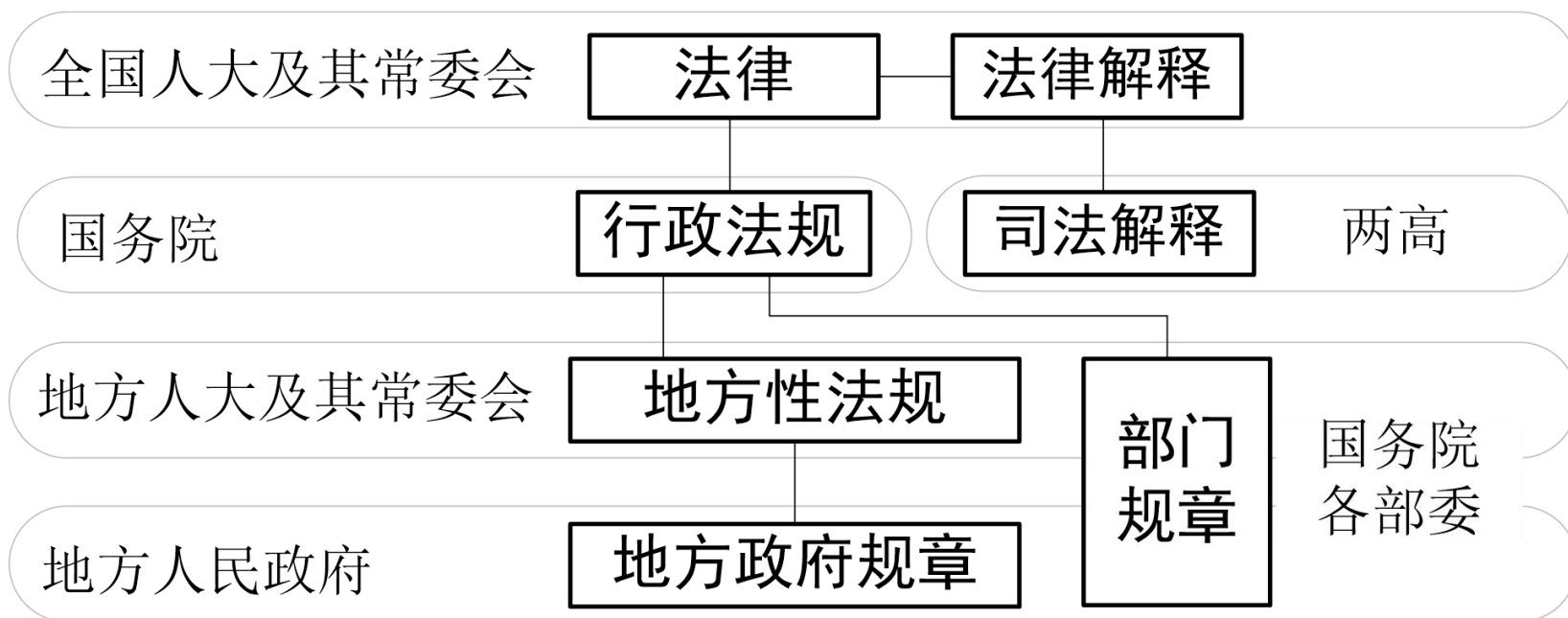


- ❖ 计算机犯罪的概念
- ❖ 计算机犯罪的特点
 - 多样化
 - 复杂化
 - 国际化
- ❖ 计算机犯罪的趋势
 - 从无意识到有组织
 - 从个体侵害到国家威胁
 - 跨越计算机本身的实施能力
 - 低龄化成为法律制约难题

我国立法体系



- ❖ 立法是网络空间治理的基础工作
- ❖ 我国采取多级立法机制



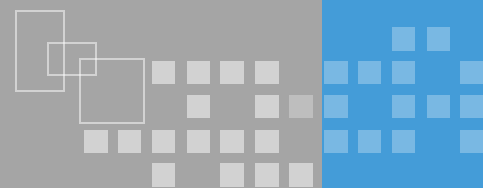
❖ 网络安全法

- 理解网络安全法出台背景；
- 理解网络安全法中定义的网络、网络安全等基本概念及网络空间主权原则；
- 了解网络运行安全制度、关键基础设施保护制度、等级保护制度、网络安全审查制度的相关要求。

❖ 网络安全相关法规建设

- 了解行政违法相关概念及相关行政处罚；
- 了解刑事责任、常见网络安全犯罪及量刑等概念；
- 了解民事违法相关概念及违法民事处罚；
- 了解国家安全法、保密法、电子签名法、反恐怖主义法、密码法中网络安全相关条款。

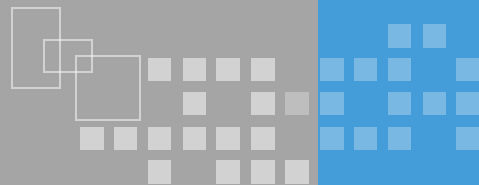
各国网络安全立法的重点制度



- ❖ 对传统的网络安全制度进行立法修正
 - 机构职责和管理制度
 - 监测预警及应急处置机制
- ❖ 对近几年涌现的新问题进行应对
 - 关键基础设施保护
 - 数据安全防护（跨境数据流动、数据泄露处置等）
 - 云计算等新技术、新业务引发的安全问题等

**网络安全立法演变为全球范围内的
利益协调与国家主权斗争**

网络安全法出台背景



- 《网络安全法》从草案发布到正式出台，共经历了**三次审议**，**两次公开征求意见和修改**。

《网络安全法》出台背景

落实国家总体安全观的重要举措

十八大以来，习总书记对加强国家网络安全工作做出了重要部署，对加强网络安全法制建设提出了明确要求

维护网络安全的客观需要

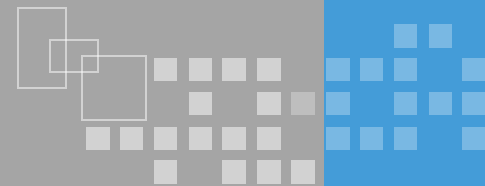
我国迫切需要建立和完善网络安全的法律制度，提高全社会的网络安全意识和网络安全保护水平

维护人民群众切身利益的迫切需要

网络侵权行为严重损害了公民、法人和其他组织的合法权益，广大人民群众迫切地呼吁加强网络空间法制建设、净化网络环境



《网络安全法》基本概念

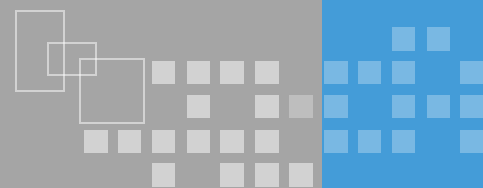


- ❖ 网络、网络安全
- ❖ 网络空间安全
- ❖ 关键信息基础设施
- ❖ 网络运营者
- ❖ 个人信息
- ❖ 网络数据
- ❖

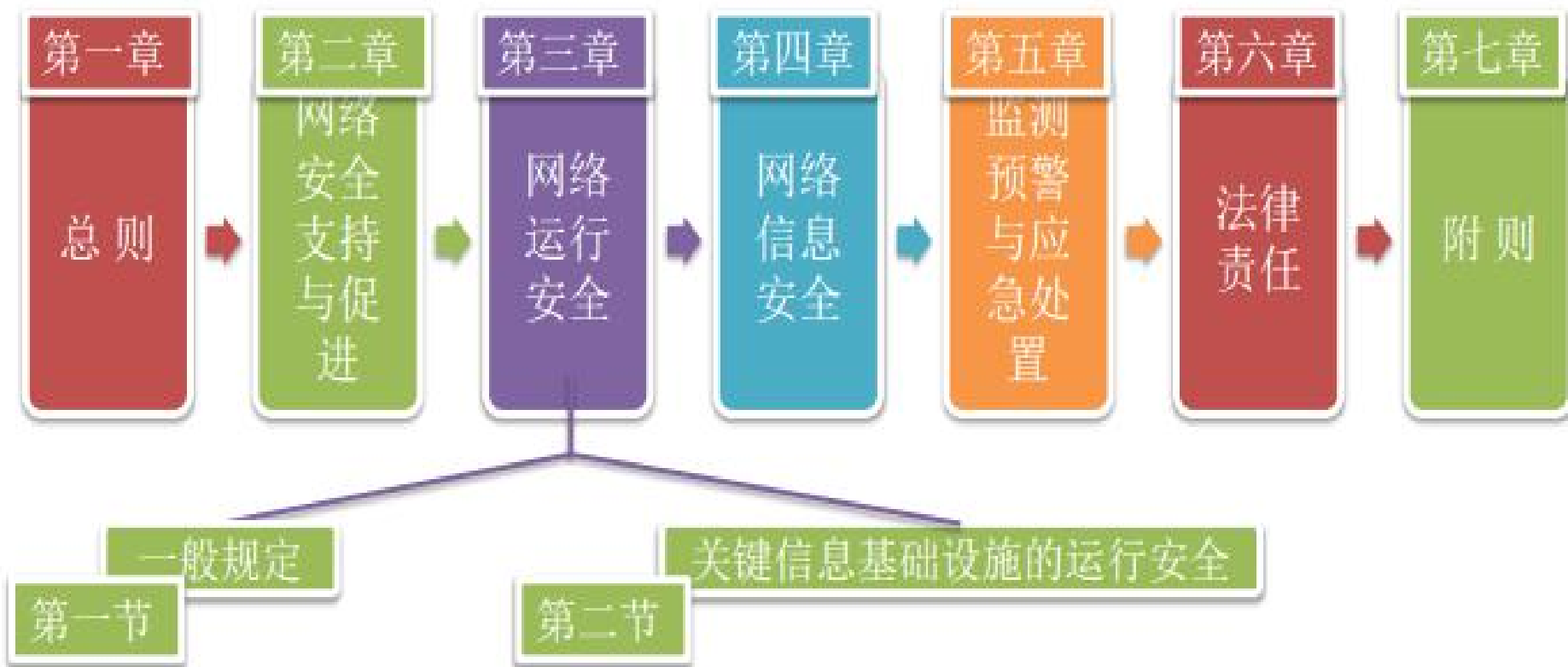
网络空间 已成为领土、领海、领空、太空之外的“**第五空间**”或人类“**第二类生存空间**”
成为国家主权延伸的新疆域



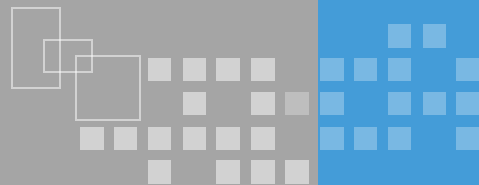
网络安全法主要结构



❖ 七章79条



第一章 总则



❖ 明确网络空间主权原则

- 作为我国网络安全治理的基本法，《网络安全法》在总则部分确立了网络主权原则，明确了网络安全管理体制和分工，及域外的适用效力。

确立网络空间主权原则

◆第1条“立法目的”中明确规定要维护我国网络空间主权。

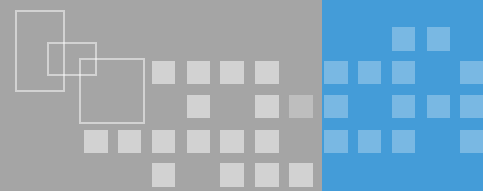
明确网络安全管理体制及职责分工

国家网信部门	国务院电信主管部门、公安部门和其他有关机关	县级以上地方人民政府有关部门
统筹协调	依法在职责范围内负责	依规定确定

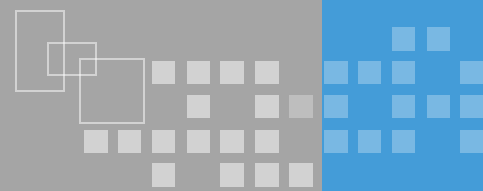
明确特定情况下的域外适用效力

对来源于境外的网络安全风险和威胁	对来源于境外的违法信息	对境外危害我国关键信息基础设施的活动
监测、防御、处置	采取措施阻断传播	追究法律责任

第二章 网络安全支持与促进



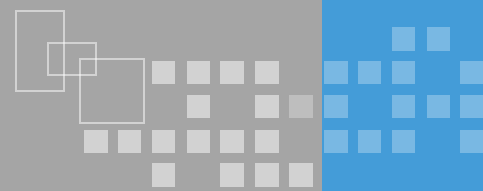
- ❖ 建立和完善网络安全标准体系建设
- ❖ 统筹规划，扶持网络安全产业（产品、服务等）
- ❖ 推动社会化网络安全服务体系建设
- ❖ 鼓励开发数据安全保护和利用技术、创新网络安全管理方式
- ❖ 开展经常性网络安全宣传教育
- ❖ 支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流



❖ 明确要求落实网络安全等级保护制度

第二十一条 国家实行**网络安全等级保护制度**。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

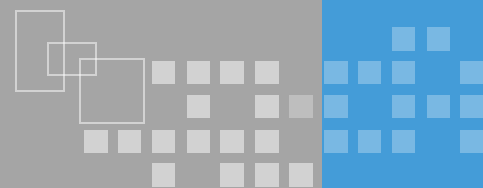
- （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
- （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；
- （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
- （四）采取数据分类、重要数据备份和加密等措施；
- （五）法律、行政法规规定的其他义务。



❖ 明确网络运营者的安全义务

- **内部安全管理**：制定内部安全管理制度和操作规程，确定网络安全负责人
- **安全技术措施**：采取防范网络安全行为的技术措施；采取监测、记录网络运行状态、网络安全事件的技术措施，留存相关的网络日志不少于六个月
- **数据安全**管理：采取数据分类、重要数据备份和加密等措施，防止网络数据泄露或者被窃取、篡改
- **网络身份管理**：办理网络接入、域名注册服务，或固定电话、移动电话等入网手续，或为用户提供信息发布、即时通讯等服务，应要求用户提供真实身份信息。
- **应急预案机制**：制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。
- **安全协助义务**：为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助

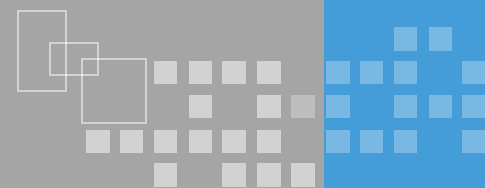
第三章 网络运行安全



❖ 明确网络产品、服务提供者的安全义务

- **强制标准义务：**网络产品、服务应当符合相关国家标准的强制性要求，不得设置恶意程序；网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供
- **告知补救义务：**网络产品、服务提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，及时告知用户，向有关主管部门报告。
- **安全维护义务：**网络产品、服务提供者应为产品、服务持续提供安全维护，在规定或者当事人约定的期限内不得终止；
- **个人信息保护：**网络产品、服务具有收集用户信息功能的，网络产品、服务提供者应向用户明示并取得同意；涉及用户个人信息的，还应遵守相关法律、行政法规中有关个人信息保护的规定。

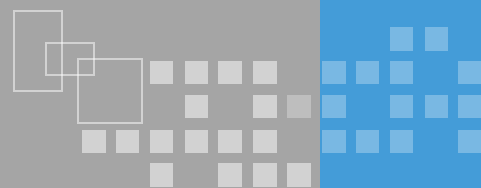
第三章 网络运行安全



❖ 明确一般性安全保护义务

- **安全信息发布**：开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。
- **禁止危害行为**：任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等。
- **信息使用规则**：网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第三章 网络运行安全



❖ 关键信息基础设施保护

1、关键信息基础设施内涵

- 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务重要行业和领域的关键信息基础设施
- 其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害**国家安全、国计民生、公共利益**的关键信息基础设施

2、关键信息基础设施外延

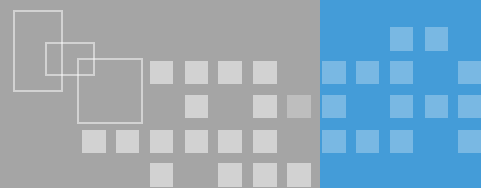
- 关键信息基础设施的具体范围由**国务院**制定
- 鼓励关键信息基础设施以外的网络运营者**自愿**参与关键信息基础设施保护体系

3、关键信息基础设施管理机制

- 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门具体负责实施**本行业、本领域**的关键信息基础设施保护工作
- **国家网信部门**统筹协调有关部门对关键信息基础设施采取安全保护措施

4、关键信息基础设施建设要求

- 确保具有支持**业务稳定、持续运行**的性能
- 安全技术措施同步规划、同步建设、同步使用

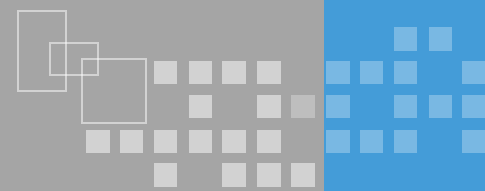


❖ 关键信息基础设施保护

5、关键信息基础设施运营者安全保护义务

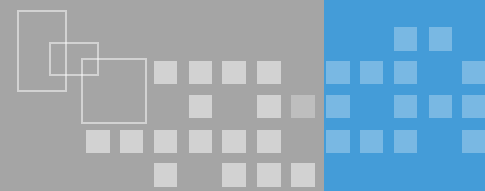
- **人员安全管理**：设置专门安全管理机构和安全管理负责人；对负责人和关键岗位的人员进行安全背景审查；定期对从业人员进行网络安全教育、培训和考核。
- **数据境内留存**：在我国境内运营中收集和产生的个人信息和重要数据应当在境内存储。确需向境外提供的，需经国家安全评估；对重要系统和数据库进行容灾备份。
- **应急预案机制**：制定网络安全事件应急预案，并定期进行演练。
- **安全采购措施**：采购网络产品和服务可能影响国家安全的，应当通过国家安全审查。应与网络产品和服务提供者签订安全保密协议。
- **风险评估机制**：自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关部门。

第三章 网络运行安全



- ❖ 关键基础设施运营中产生的数据必须**境内存储**
- ❖ 2017年04月10日国家互联网信息办公室发布关于《个人信息和重要数据出境安全评估办法（征求意见稿）》公开征求意见的通知。明确了
 - 个人信息和重要数据出境的范围
 - 有50万人以上的个人信息
 - 数据量超过1000GB
 - 7大重要领域数据等
 - 数据出境评估原则
 - 评估7个方面主要内容

第三章 网络运行安全



❖ 明确我国实行网络安全审查制度

第三十五条

关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

- ❖ 2017年05月02日中央网信办正式发布《网络产品和服务安全审查办法（试行）》。其中就审查的目的、需要审查的网络产品和服务的范围、网络安全审查的管理部门（网络安全审查委员会）、审查的机构（国家统一认定网络安全审查第三方机构）和对党政机关和重点行业的审查工作提出要求。并于2017年6月1日同《网络安全法》一同实施。

第四章 网络信息安全

❖ 重视对个人信息保护

保护规范

原则：合法、正当、必要（第41条）

规则：吸收了国际通行规则

规则透明：公开规则、获得同意（第41条）

目的限制：不得超范围收集、违法和违约收集（第41条）

安全保密：不得泄露毁损、预防措施、补救措施（第40、42条）

删除改正：删除违法、违约信息、改正有误信息（第43条）

规范主体

网络运营者、任何个人和组织、负有网络安全监督管理职责的部门及其工作人员

网络运营者

安全保密、知情同意、目的限制、删除改正、

个人和组织

不得窃取、非法出售个人信息

监督部门

保密、不得泄露出售

第四章 网络信息安全

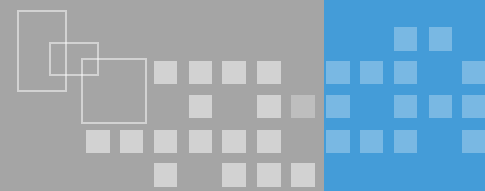
❖ 规范信息管理



第四章 网络信息安全

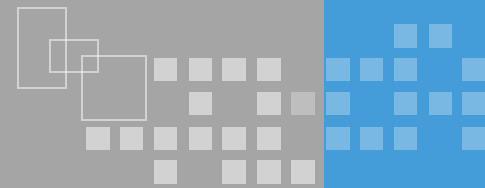
❖ 确定信息管理中相关职责





❖ 2017年05月02日国家互联网信息办公室正式发布《**互联网新闻信息服务管理规定**》（**国信办1号令**），于6月1日同《网络安全法》一起实施。规范了：

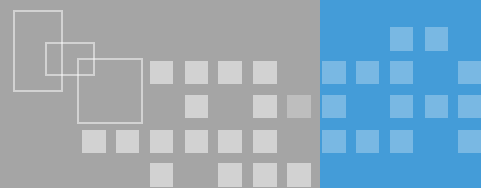
- 互联网新闻信息服务的范围
- 互联网新闻信息服务的6项许可条件
- 互联网新闻信息服务提供者的责任义务
- 网信部门对互联网新闻信息服务的监督检查要求
- 相关法律责任



❖ 同日国家互联网信息办公室一并发布《**互联网信息服务内容管理行政执法程序规定**》（**国信办2号令**），于6月1日同《网络安全法》一起实施。规范了：

- 互联网信息服务内容管理部门行政执法依据
- 管辖范围
- 立案流程
- 调查取证过程
- 听证及约谈机制
- 处罚决定及执行办法等

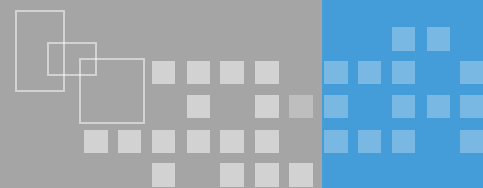
第五章 监测预警与应急处置



❖ 工作制度化、法制化

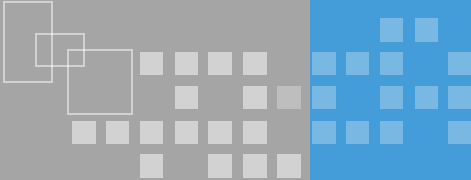
责任主体	具体制度
国家网信部门	<ul style="list-style-type: none">统筹网络安全信息收集、分析和通报，统一发布网络安全监测预警信息；制定网络安全事件应急预案，定期组织演练。
负责关键基础设施安全保护工作部门	<ul style="list-style-type: none">建立健全本行业、本领域的网络安全监测预警和信息通报制度，按照规定报送预警信息；制定本行业、本领域的网络安全事件应急预案，定期组织演练。
省级以上人民政府有关部门	<ul style="list-style-type: none">网络安全事件发生的风险增大时，采取信息报送、网络安全风险信息评估、向社会预警等措施；按照规定程序及权限对网络运营者法定代表人进行约谈
网络运营者	<ul style="list-style-type: none">采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息；按照省级以上人民政府要求进行整改，消除隐患

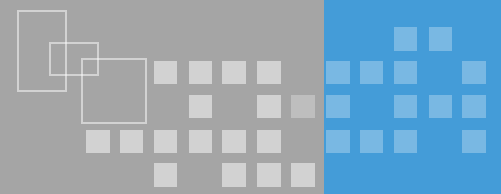
第六章 法律责任



❖ 对违反《网络安全法》的行为，第六章规定了民事责任、行政责任、刑事责任



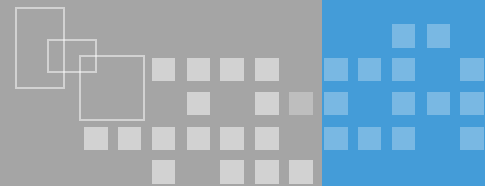
- 
- ❖ 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，加强在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了一部法律草案，并于 7 月 6 日起在网上全文公布，向社会公开征求意见，这部法律草案是（）
- ❖ A. 《中华人民共和国保守国家秘密法（草案）》
 - ❖ B. 《中华人民共和国网络安全法（草案）》
 - ❖ C. 《中华人民共和国国家安全法（草案）》
 - ❖ D. 《中华人民共和国互联网安全法（草案）》



- ❖ 为了进一步提高信息安全的保障能力和防护水平，保障和促进信息化建设的健康发展，公安部等四部门联合发布《关于信息安全等级保护工作的实施意见》（公通[2004]66 号），对等级保护工作的开展提供宏观指导和约束。明确了等级保护工作的基本内容、工作要求和实施计划，以及各部门工作职责分工等。关于该文件，下面理解正确的是（）
- ❖ A. 该文件是一个由部委发布的政策性文件，不属于法律文件
- ❖ B. 该文件适用于 2004 年的等级保护工作。其内容不能约束到 2005 年及之后的工作
- ❖ C. 该文件是一个总体性指导文件，规定了所有信息系统都要纳入等级保护定级范围
- ❖ D. 该文件适用范围为发文的这四个部门，不适用于其他部门和企业等单位



- ❖ 行政法相关法规
- ❖ 民法相关法规
- ❖ 刑法相关法规
 - 出售或者提供公民个人信息罪、非法侵入计算机信息系统罪、网络服务渎职罪等
- ❖ 其他网络安全相关法规及条款
 - 国家安全法
 - 保密法
 - 电子签名法
 - 反恐怖主义法
 - 密码法

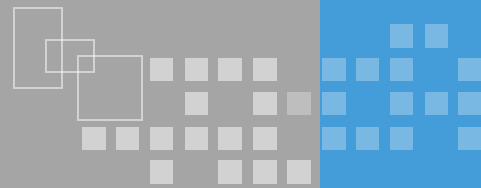


❖ 国家网络空间安全战略

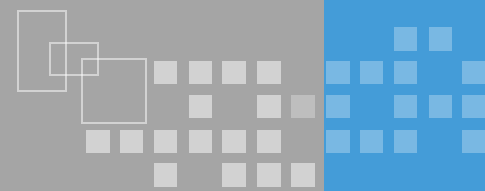
- 了解国家 《网络空间安全战略》中总结的七种新机遇、六大严峻挑战及建设网络强国的战略目标；
- 了解《国家网络空间战略》提出的四项基本原则和九大任务；

❖ 国家网络安全等保政策

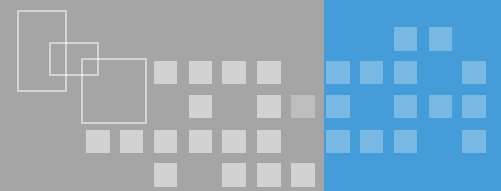
- 了解我国网络安全等级保护相关政策。



- ❖ 七种新机遇
- ❖ 六大严峻挑战
- ❖ 发展战略目标
- ❖ 四项原则
- ❖ 九大任务



- ❖ 《中华人民共和国计算机信息系统安全保护条例》规定了计算机系统实现安全等级保护
- ❖ GB 17859正式细化等级保护要求，**划分五个级别**
- ❖ 《关于信息安全等级保护工作的实施意见的通知》规定等级保护指导思想、原则和要求。定级从信息和信息系统的业务重要性及遭受破坏后的影响出发
- ❖ 网络安全法明确我国实行网络安全等级保护制度

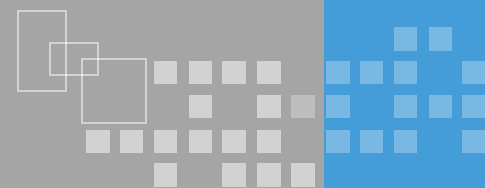


❖ 道德约束

- 了解道德的概念、道德与法律的差异；
- 理解道德约束相关概念。

❖ 职业道德准则

- 理解信息安全从业人员遵守职业道德的重要性；
- 了解目前国际团体和组织制作的职业道德规范文件；
- 理解《CISP职业道德准则》的要求；



❖ 道德的概念

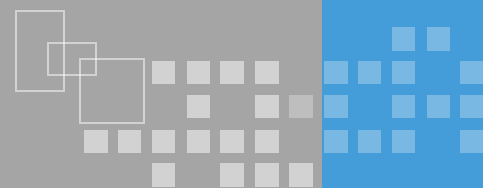
- 一定社会或阶级用以调整人们之间利益关系的行为准则，也是评价人们行为善恶的标准

❖ 道德和法律

- 道德没有严谨的结构体系，法律是国家意志统一体系，有严密的逻辑

❖ 道德约束

- 道德约束是建立在完善的法律基础上
- 惩戒性条款的管理制度是组织内部建立职业道德约束的有效手段之一
- 培训与教育是获取的增强员工道德意识的途径



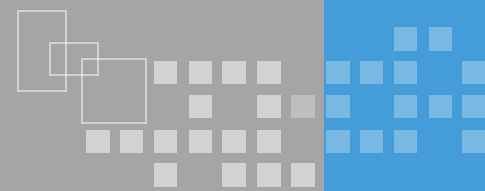
❖ 职业道德的概念

❖ 著名的计算机职业伦理守则

- 美国计算机学会职业伦理守则、英国计算机学会伦理守则、计算机伦理十诫

❖ CISP职业道德准则

- 维护国家、社会和公众的信息安全
- 诚实守信、遵纪守法
- 努力工作，尽职尽责
- 发展自身，维护荣誉

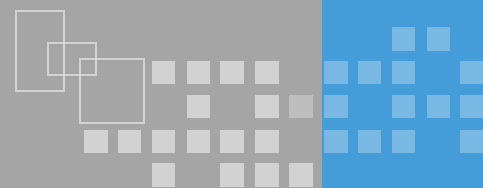


❖ 信息安全标准基础

- 了解标准的基本概念及标准的作用、标准化的特点及原则等；
- 了解国际信息安全标准化组织和我国信息安全标准化组织；
- 了解我国标准分类及信息安全标准体系。

❖ 我国信息安全标准

- 了解我国信息安全标准体系分类及基础标准、技术与机制、管理与服务标准、测评标准构成；

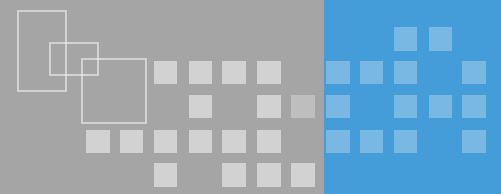


❖ 标准

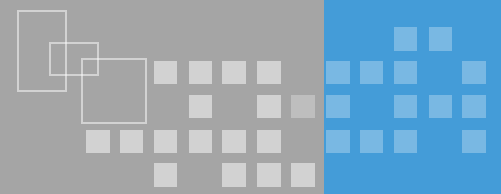
- 为了在一定范围内获得最佳秩序，经协商一致制定并由公认机构批准，共同使用的和重复使用的一种规范性文件

❖ 标准类型

- 国际标准
- 国家标准
- 行业标准
- 地方标准



- ❖ 标准化：为了在一定范围内获得最佳秩序，对现实问题或潜在问题制定共同使用和重复使用的条款的活动
- ❖ 标准化的基本特点
 - 标准化是一项活动
 - 标准化的对象：物、事、人
 - 标准化是一个动态的概念
 - 标准化是一个相对的概念
 - 标准化的效益只有应用后才能体现
- ❖ 标准化工作原则：简化、统一、协调、优化

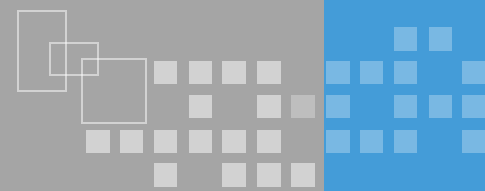


❖ 主要国际标准化组织

- 国际标准化组织（ISO）
- 国际电工委员会（IEC）
- Internet工程任务组（IETF）
- 国际电信联盟（ITU）及国际电信联盟远程通信标准化组织（ITU-T）

❖ 国家标准化组织（美国）

- 美国国家标准化协会（ANSI）
- 美国国家标准技术研究院（NIST）

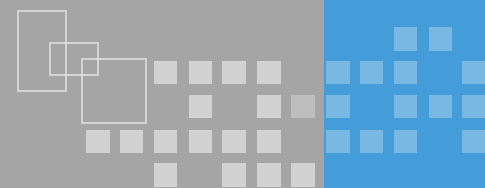


❖ 中国国家标准化管理委员会

- 是我国最高级别的国家标准机构

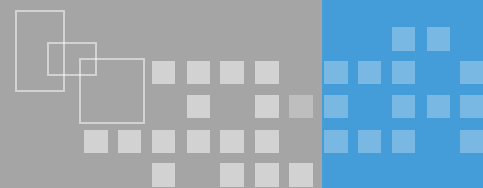
❖ 全国信息安全标准化技术委员会（TC260）

- 1984年，成立数据加密技术分委员，后来改为信息技术安全分技术委员会
- 2002年4月，为加强信息安全标准的协调工作，国家标准委决定成立全国信息安全标准化技术委员会（信安标委，TC260），由国家标准委直接领导，对口ISO/IEC JTC1 SC27
- 国家标准化管理委员会高新函[2004]1号文决定：自2004年1月起，各有关部门在申报信息安全国家标准计划项目时，必须经信息安全标委会提出工作意见，协调一致后由信息安全标委会组织申报；在国家标准制定过程中，标准工作组或主要起草单位要与信息安全标委会积极合作，并由信息安全标委会完成国家标准送审、报批工作



❖ TC260组织结构





❖ GB 强制性国家标准

- 一经颁布必须贯彻执行，违反则构成经济或法律方面的责任

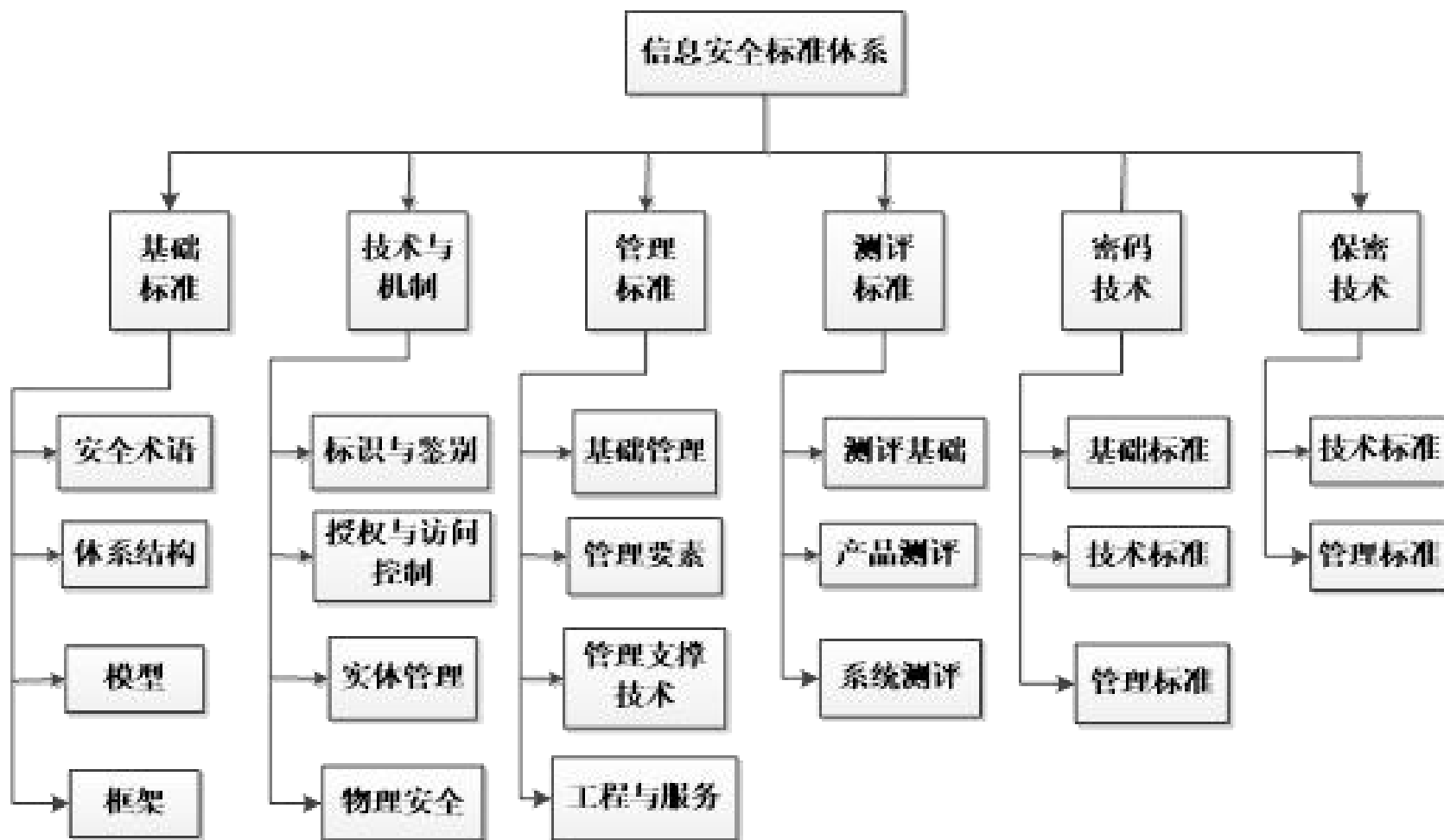
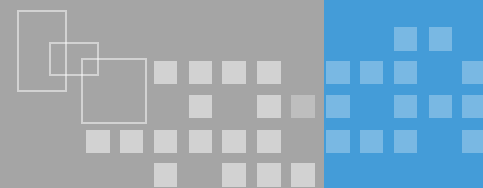
❖ GB/T 推荐性国家标准

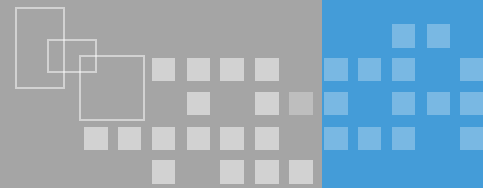
- 自愿采用的标准，共同遵守的技术依据，严格贯彻执行

❖ GB/Z 国家标准指导性技术文件

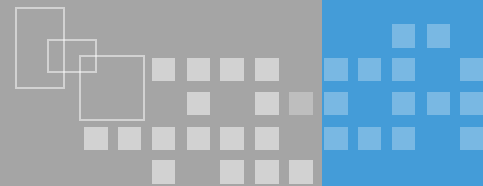
- 由于技术发展过程中或其他理由，将来可能达成一致意见指导性技术文件
- 实施后3年内必须进行复审

我国信息安全标准体系

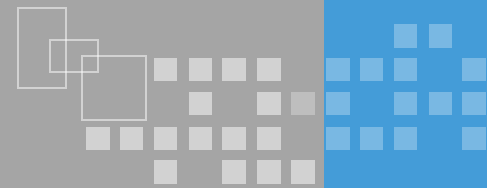




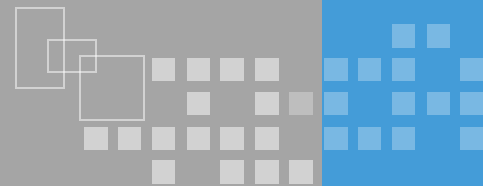
- ❖ 安全术语类
- ❖ 测评基础类
- ❖ 管理基础类
- ❖ 物理安全类
- ❖ 安全模型类
- ❖ 安全体系架构类



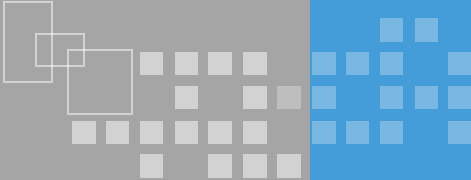
- ❖ 密码技术
- ❖ 鉴别机制
- ❖ 授权机制
- ❖ 电子签名
- ❖ 公钥基础设施
- ❖ 通信安全技术
- ❖ 涉密系统通用技术要求



- ❖ 涉密服务
- ❖ 安全控制与服务
- ❖ 网络安全管理
- ❖ 行业/领域安全管理

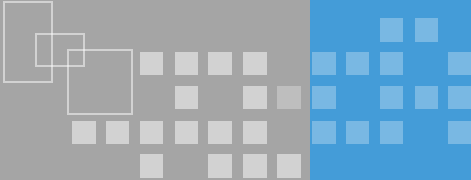


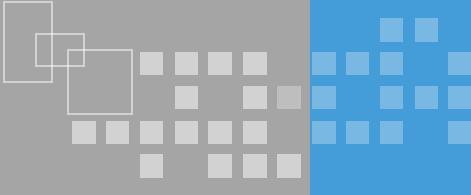
- ❖ 密码产品
- ❖ 通用产品
- ❖ 安全保密产品
- ❖ 通用系统
- ❖ 涉密信息系统
- ❖ 通信安全
- ❖ 政府安全检查
- ❖ 安全能力评估

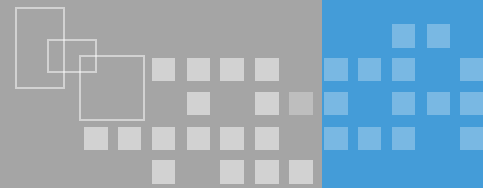
- 
- ❖ 在以下标准中，属于推荐性国家标准的是？
 - ❖ A. GB/T XXXX.X-200X B. GB XXXX--200X
 - ❖ C. DBXX/T XXX-200X D. GB/Z XXX-XXX-200X

QB是企业标准，

GB是国家标准，T意思为推荐即推荐标准不是强制标准，Z为指导性标准

- 
- ❖ 标准是标准化活动的成果，是为了在一定范围内获得最佳秩序，经协调一致制定并由公认机构批准，共同重复使用的一上规范性文件。关于标准和标准化，以下选项中理解错误的是（）
 - ❖ A. 标准化是一项活动，标准化工作的主要任务是定标准、组织实施以及对标准的实施进行监督，主要作用是为了预期的目的而改进产品、过程或服务的实用性，防止壁垒，促进合作
 - ❖ B. 标准化的对象不应是孤立的一件事或一个事物，而是共同的、可重复的事物、标准化的工作同时也具有动态性，即应随着科学的发展和社会的进步而不断修订标准
 - ❖ C. 标准在国际贸易中有着重要作用，一方面，标准能打破技术壁垒，促进国际间的经贸发展和科学、技术、文化交流和合作；另一方面，标准化也能成为新的技术壁垒，起到限制他国产品出口，保护本国产业的目的
 - ❖ D. 标准有着不同的分类，我国将现有标准分为强制标准、推荐标准和事实性标准三类，国家标准管理机构对三类标准通过不同字头的方式分别编号后公开布

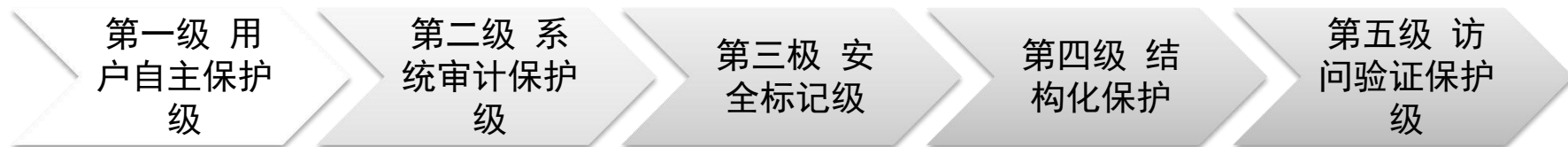
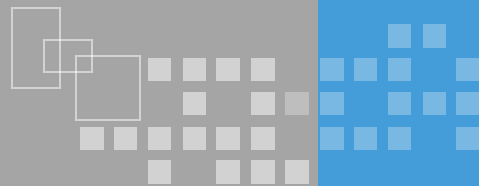
- 
- ❖ 自2004 年1 月起，国内各有关部门在申报信息安全国家标准计划项目时，必须经由以下哪个组织提出工作意见，协调一致后由该组织申报。
 - ❖ A. 全国通信标准化技术委员会(TC485)
 - ❖ B. 全国信息安全标准化技术委员会(TC260)
 - ❖ C. 中国通信标准化协会(CCSA)
 - ❖ D. 网络与信息安全技术工作委员会



❖ 等级保护标准族

- 了解网络安全等级保护标准体系；
- 掌握等级保护实施流程中定级、备案的工作要求并了解等级保护整改、测评相关要求；
- 了解等级保护2.0的相关变化。

等级保护定义



--定义

- 等级保护全称为“信息系统安全等级保护”，现改为“**网络安全等级保护**”，是指对网络和信息系统按照**重要性等级分级别保护**的一种工作；根据网络与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，由低到高被划分为**五个安全保护等级**

--概括说明

- 系统重要程度有多高，安全保护就应当有多强，**既不能保护不足，也不能过度保护。**

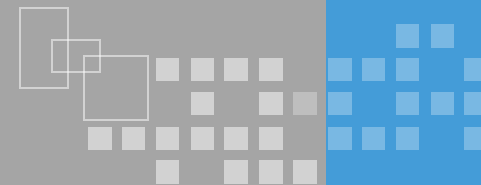
--等级保护对客户意义

- 遵循客观规律，网络安全的**等级是客观存在的**
- 有利于突出重点，**加强安全建设和管理**
- 有利于控制信息安全建设的成本，**平衡安全建设与成本**

--等级保护对国家意义

- **制度**：是为了构建国家信息安全保障体系。
- **抓手**：提高信息系统安全防护能力。
- **带有很强技术性的国家风险管控行为**

等级保护管理组织



指导监管部门：
国家等保工作 开展、推进、指导。



技术支撑部门：
国家等保标准制定、修订、培训、技术指导以及全国测评单位管理。



(国) - 001	公安部信息安全等级保护评估中心
(国) - 002	国家信息技术安全研究中心
(国) - 003	中国信息安全测评中心

国家测评机构

(国) - 004	电力行业信息安全等级保护测评中心
(国) - 005	中国金融电子化公司测评中心
(国) - 006	教育信息安全等级保护测评中心
(国) - 007	国家广播电影电视总局广播电视信息安全测评中心

行业测评机构

(津) - 002	天津市先特网络软件系统有限公司
(冀) - 003	河北恒讯达信息科技有限公司
(津) - 003	天津优扬科技有限公司
(冀) - 005	石家庄星安信息安全测评技术有限公司
(晋) - 001	太原清众鑫科技有限公司
(晋) - 002	中国信息安全测评中心山西测评中心
(晋) - 003	山西省软件测评服务中心
(蒙) - 001	内蒙古信元信息安全评测有限责任公司

地方测评机构

新等级保护标准体系

新等级保护标准变化

网络安全等级保护定级指南（修订）

网络安全等级保护实施指南（修订）

网络安全等级保护基本要求（修订）

网络安全等级保护安全技术要求（修订）

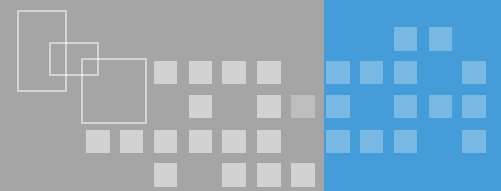
网络安全等级保护测评过程指南（修订）

网络安全等级保护测评过程指南（新立）

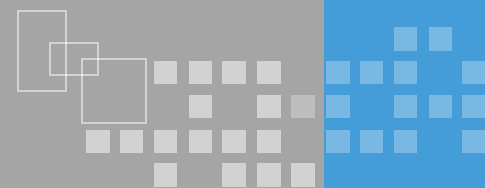
网络安全等级保护测评机构能力要求和评估规范（新立）

安全管理中心技术要求（新立）



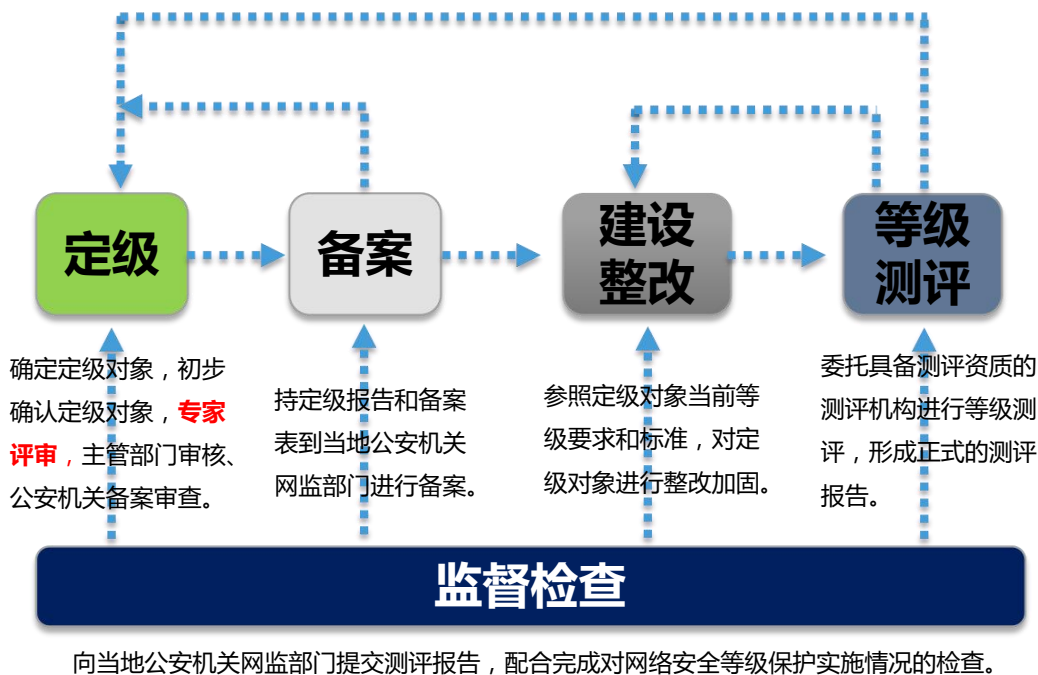
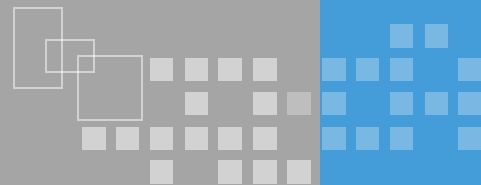


- ❖ 安全等级类：主要对如何进行信息系统定级做出指导
 - GB/T22240-2008 《信息安全技术 信息系统安全保护等级保护定级指南》
 - 各类行业定级准则
- ❖ 方法指导类：对如何开展等级保护工作做了详细规定
 - GB/T25058-2010 《信息安全技术 信息系统安全等级保护实施指南》
 - GB/T25070-2010 《信息系统等级保护安全设计技术要求》等



- ❖ 状况分析类：对如何开展等级保护测评工作做出了详细规定
 - GB/T28448-2012 《信息安全技术 信息系统安全等级保护测评要求》
 - GB/T28449-2012 《信息安全技术 信息系统安全等级保护测评过程指南》等
- ❖ 基线要求类：分技术类、管理类和产品类等标准，分别对某些专门技术、管理和产品的进行要求
 - 例如：GB/T22239-2008 《信息安全技术 信息系统安全等级保护基本要求》、GB/T20271-2006 《信息系统通用安全技术要求》、GB/T21052-2007 《信息系统物理安全技术要求》

等级保护主要工作流程



定级

步骤：确定定级对象，初步确认定级对象，专家评审，主管部门审核、公安机关备案审查。



备案

持定级报告和备案表到当地公安机关网监部门进行备案



建设整改

参照信息系统当前等级要求和标准，对信息系统进行整改加固



等级测评

委托具备测评资质的测评机构对信息系统进行等级测评，形成正式的测评报告



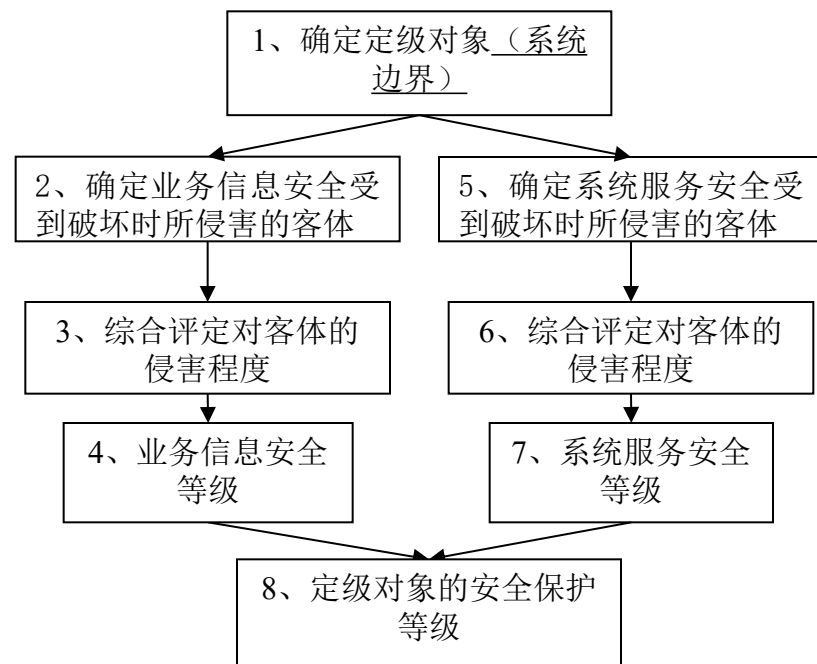
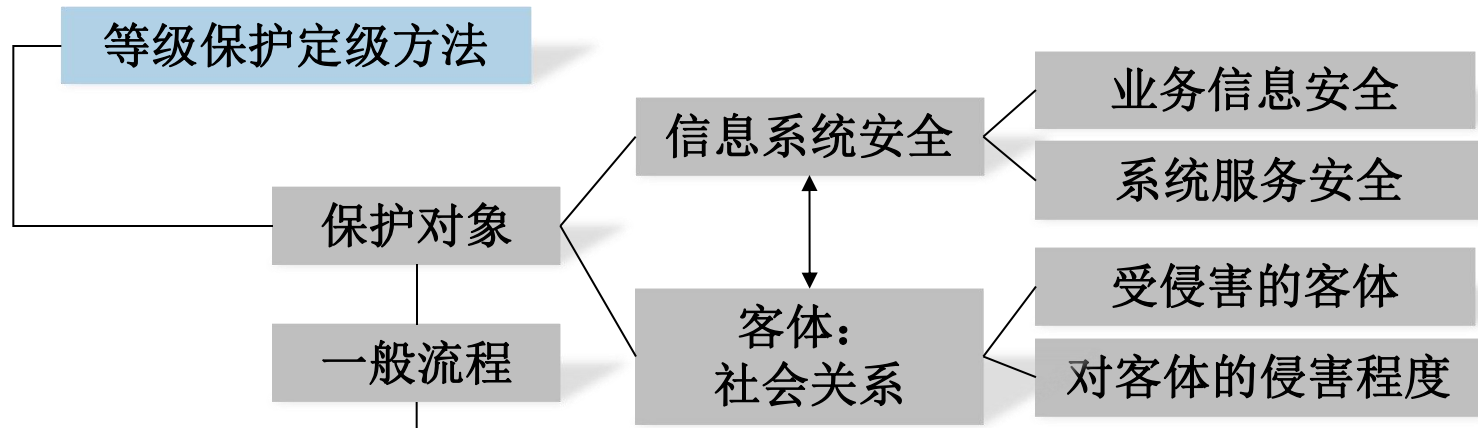
监督检查

向当地公安机关网监部门提交测评报告，配合完成对信息安全等级保护实施情况的检查。

监督检查是保护能力不断提高的保障

定级与备案

等级保护定级方法

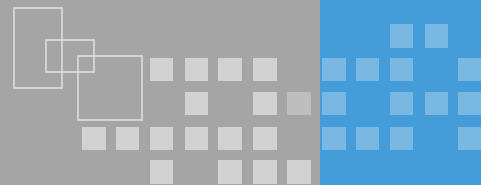


$$8 = \text{MAX}(4, 7)$$

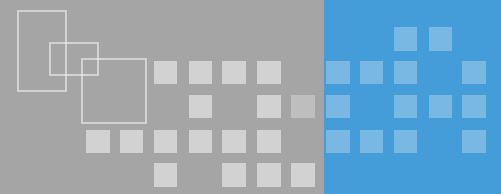
等级确定

保护对象受到破坏时 受侵害的客体	对客体的侵害程度		
	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	第三级
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

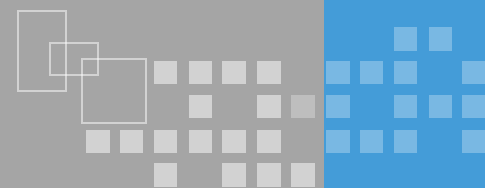
定级与备案



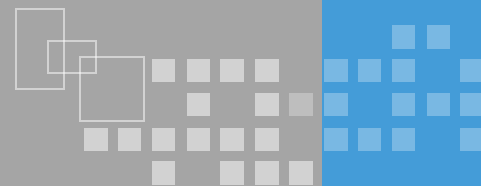
- ❖ **第一级（自主保护级）**：一般适用于小型私营、个体企业、中小学，乡镇所属信息系统、县级单位中一般的信息系统。
- ❖ 信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
- ❖ **第二级（指导保护级）**：一般适用于县级其他单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
- ❖ **第三级（监督保护级）**：一般适用于地市级以上国家机关、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。
- ❖ 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（强制保护级）**：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。
- ❖ 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（专控保护级）**：一般适用于国家重要领域、重要部门中的极端重要系统。
- ❖ 信息系统受到破坏后，会对国家安全造成特别严重损害。



- ❖ 目的：发现系统当前安全状况与《等级保护基本要求》之间差距，指导下一步整改工作
- ❖ 流程：差距分析流程与等级保护测评一致
- ❖ 报告：在完成差距分析后一般形成《等级保护差距分析报告》，格式一般参考《等级保护测评报告》，为下一阶段开展等级保护安全建设整改工作提出建设整改需求。



- ❖ 依据：GB/T25070-2010《信息系统等级保护安全设计技术要求》
- ❖ 流程：依据《等级保护差距分析报告》中提出的安全建设整改需求，设计《等级保护安全建设整改方案》，并根据单位实际的资金、技术、人员配备情况分阶段地开展等级保护建设整改工作。
- ❖ 报告：建设整改前，需要编制《等级保护安全建设整改方案》，提出建设整改目标和步骤。在完成整改后，由建设单位开展验收工作，验证是否达到方案要求



GB/T22239.1 网络安全等级保护基本要求 第1部分 安全通用要求

GB/T
22239.2
第2部分 云计算安全扩展要求

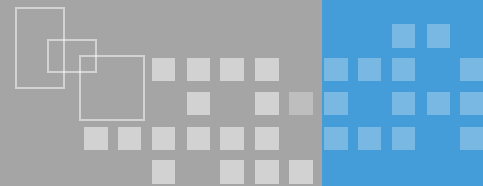
GB/T
22239.3
第3部分 移动互联安全扩展要求

GB/T
22239.4
第4部分 物联网安全扩展要求

GB/T
22239.5
第5部分 工业控制安全扩展要求

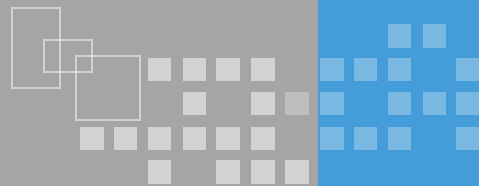
GB/T
22239.6
第6部分 大数据安全扩展要求

等级保护扩展要求



- ❖ 云计算安全要求
- ❖ 移动互联网安全
- ❖ 物联网安全
- ❖ 工业控制系统安全

等保2.0与1.0的变化



名称变化

《信息安全技术 **信息系统** 安全等级保护基本要求》

上升到了网络空间安全层面

《信息安全技术 **网络安全** 安全等级保护基本要求》

定级对象变化

信息系统

等级保护对象：基础信息网络、云计算平台、大数据平台、物联网系统、工业控制系统、采用移动互联技术的网络等

安全要求变化

安全要求

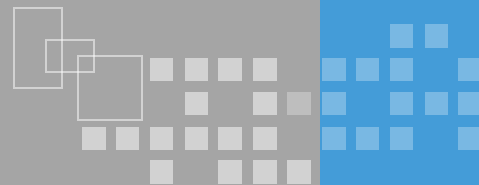
安全通用要求与安全扩展要求

分类结构变化

技术（物理、网络、主机、应用、数据）+ 管理

技术（物理环境、一中心三防护）+ 管理

等保2.0测评的变化



等保1.0

- 第三级系统每年一次，第四级系统每半年一次。

等保2.0

- 第三级以上系统每年一次。

测评周期

等保1.0

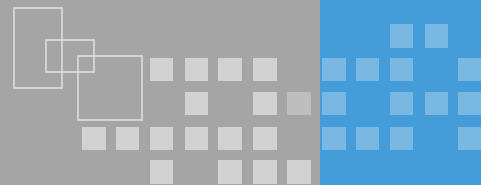
- 60分以上基本符合。

等保2.0

- 75分以上基本符合。

测评结果

等保2.0与1.0的变化-体系结构



整体变化

技术

管理

□ 安全控制域划分上有较大变化，原有十个安全域整合为八个后又整合为十个

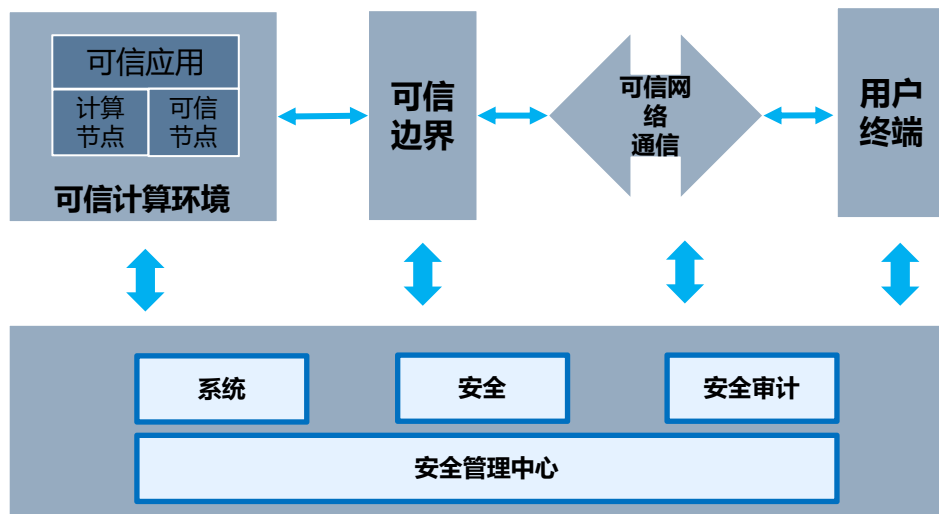
□ 定义上更精确，内涵更为丰富。

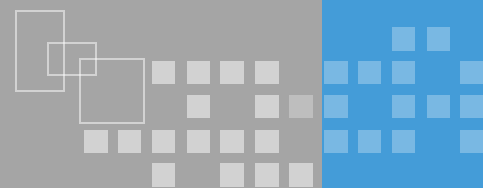
控制措施分类结构的变化					
旧标准（2008）等保 1.0			标准意见稿		新标准
技术要求	物理安全	————→	物理和环境安全	————→	安全物理环境
	网络安全	————→	网络和通信安全	————→	安全通信网络
	主机安全	————→	设备和计算安全	————→	安全区域边界
	应用安全	————→	应用和数据安全	————→	安全管理中心
	数据安全	————→		————→	安全计算环境
管理要求	安全管理制度	————→	安全策略和管理制度	————→	安全管理制度
	安全管理机构	————→	安全管理机构和人员	————→	安全管理机构
	人员安全管理	————→		————→	安全管理人员
	系统建设管理	————→	安全建设管理	————→	安全建设管理
	系统运维管理	————→	安全运维管理	————→	安全运维管理

等保2.0与1.0的变化--新增可信计算

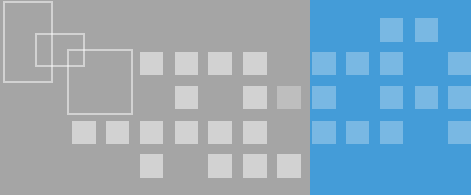
等保2.0加强可信体系作为重要思想，解决了GB 17859-1999在等级划分准则提出的“可信计算基”要求

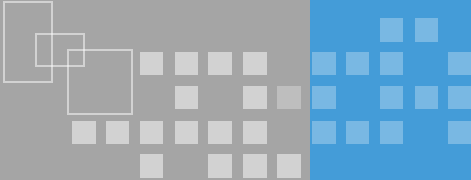
- 安全通信网络可信验证：可基于可信根对**通信设备**的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证
- 安全区域边界可信验证：可基于可信根对**边界设备**的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证
- 安全计算环境可信验证：可基于可信根对**计算设备**的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证

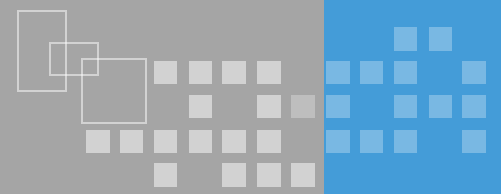




- ❖ 网络安全法律体系建设
 - 计算机犯罪、信息安全等基本概念
 - 我国立法体系及网络安全法
- ❖ 国家网络安全政策
 - 网络空间安全国家战略
 - 网络安全法相关保护
- ❖ 网络安全道德与准则
- ❖ 网络安全标准
 - 标准与标准化
 - 标准机构与标准体系
 - 国家网络安全标准体系

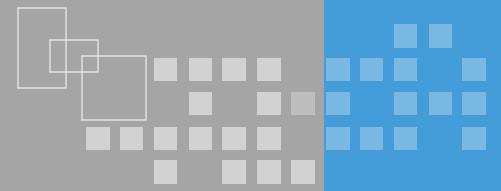
- 
- ❖ 为推动我国信息安全等级保护工作，我国制定和发布了信息安全等级保护标准其中、属于国家制定标准，且在信息安全等级保护标准体系中处于基础地位的是（）
 - ❖ A. GB/T 22239-2008 《信息系统安全等级保护基本要求》
 - ❖ B. GB/T 22240-2008 《信息系统安全等级保护等级定级指南》
 - ❖ C. GB/T 25058-2010 《信息系统安全等级保护实施指南》
 - ❖ D. GB 17859-1999 《计算机信息系统安全保护等级划分准则》

- 
- ❖ 以下哪项制度或标准作为我国的一项基础制度加以推行，并且有一定强制性，其实施的主要目标是有效地提高我国信息和信息系统安全建设的整体水平，重点保障基础信息网络和重要信息系统的安全（ ）
 - ❖ A. 信息安全管理体制
 - ❖ B. 信息安全等级保护
 - ❖ C. NIST SP800
 - ❖ D. ISO 270000 系列



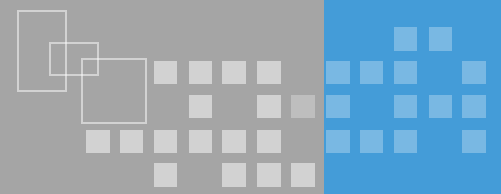
等级保护实施流程正确的是：

- ❖ A 定级、备案、安全建设、测评、监督检查
- ❖ B 定级、测评、备案、安全建设、监督检查
- ❖ C 定级、安全建设、备案、测评、监督检查
- ❖ D 备案、定级、安全建设、测评、监督检查



等级保护定级阶段主要包括哪2个步骤

- ❖ A、系统识别与描述、等级确定
- ❖ B、系统描述、等级确定
- ❖ C、系统识别、系统描述
- ❖ D、系统识别与描述、等级分级



以下关于等级保护的描述正确的是

- ❖ A 等级保护共分五个级别
- ❖ B 我国的等级保护工作由工信部主管
- ❖ C 我国已经针对等级保护出台了专门的法律
- ❖ D 等级保护的各个级别必须由实施单位和主管部门共同完成



谢谢，请提问题！