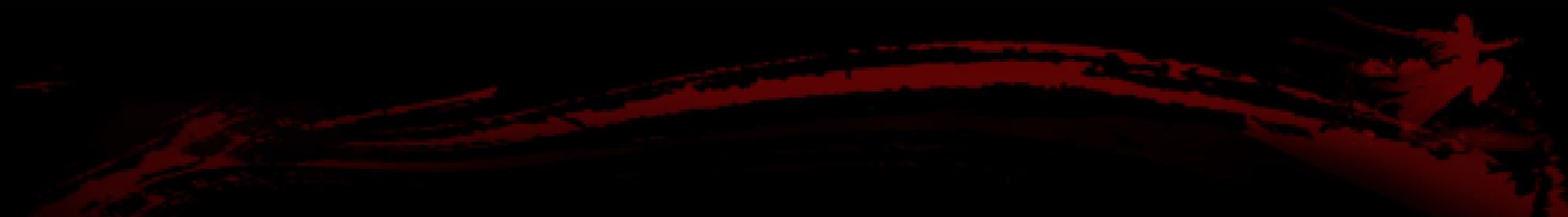




网络安全等级保护体 系标准及监管要求

姓名

单位职务





目录

◆ 网络安全等级保护2.0概述

◆ 等保2.0的特点

◆ 主要标准介绍

◆ 其他

等级保护是法律要求

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。

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门**责令改正，给予警告**；拒不改正或者导致危害网络安全等后果的，**处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款**。



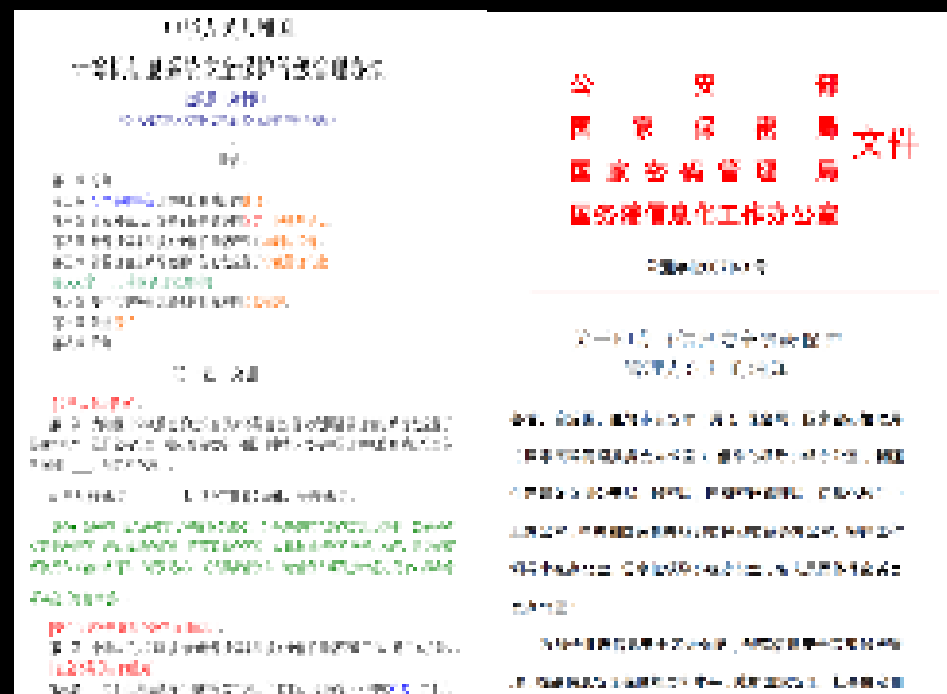
等级保护要干什么

等保 制度 精髓

以所承载的业务应用的“**社会重要性**”来确定安全保护等级；
国家信息安全风险控制行为，体现国家管理意志，构建国家信息安全保障体系，维护国家不同等级的系统采用不同的“**基线**”予以保护并家安全、公众利益，保护重要信息系统和关键基础设施，促进信息化发展；
对其实施不同的监管；
创造性地提出了适合我国国情的信息安全保护流程和方法。

等级保护的关键所在

- 保护数据安全是初衷
- 重要性定级是首要环节
- 分等级保护和监管是核心
- 国家要求和业务需求结合



等级保护取得的成绩

- 整体提高了全国人民的信息安全意识
- 有效推动了信息安全在各个行业蓬勃开展
- 帮助运营使用单位梳理了信息系统，业务应用
- 按行业、分部门逐级明确落实信息安全责任
- 为构建国家信息安全保障体系打下坚实基础
- 有力保障了国家安全、公共秩序、促进了信息化发展

新形势 新变化 新干法

新形势、新变化

云、大、物、移、工
新技术、新应用、新业态
网络空间成为新的主权疆土
当务之急保护关键基础设施

等级保护2.0

- 安全法颁布实施
- CII等级保护策略
- 等保2.0的新标准体系及内容

等级保护工作从1.0迈向2.0

管理策略、技术标准提出新要求

什么是等级保护2.0？

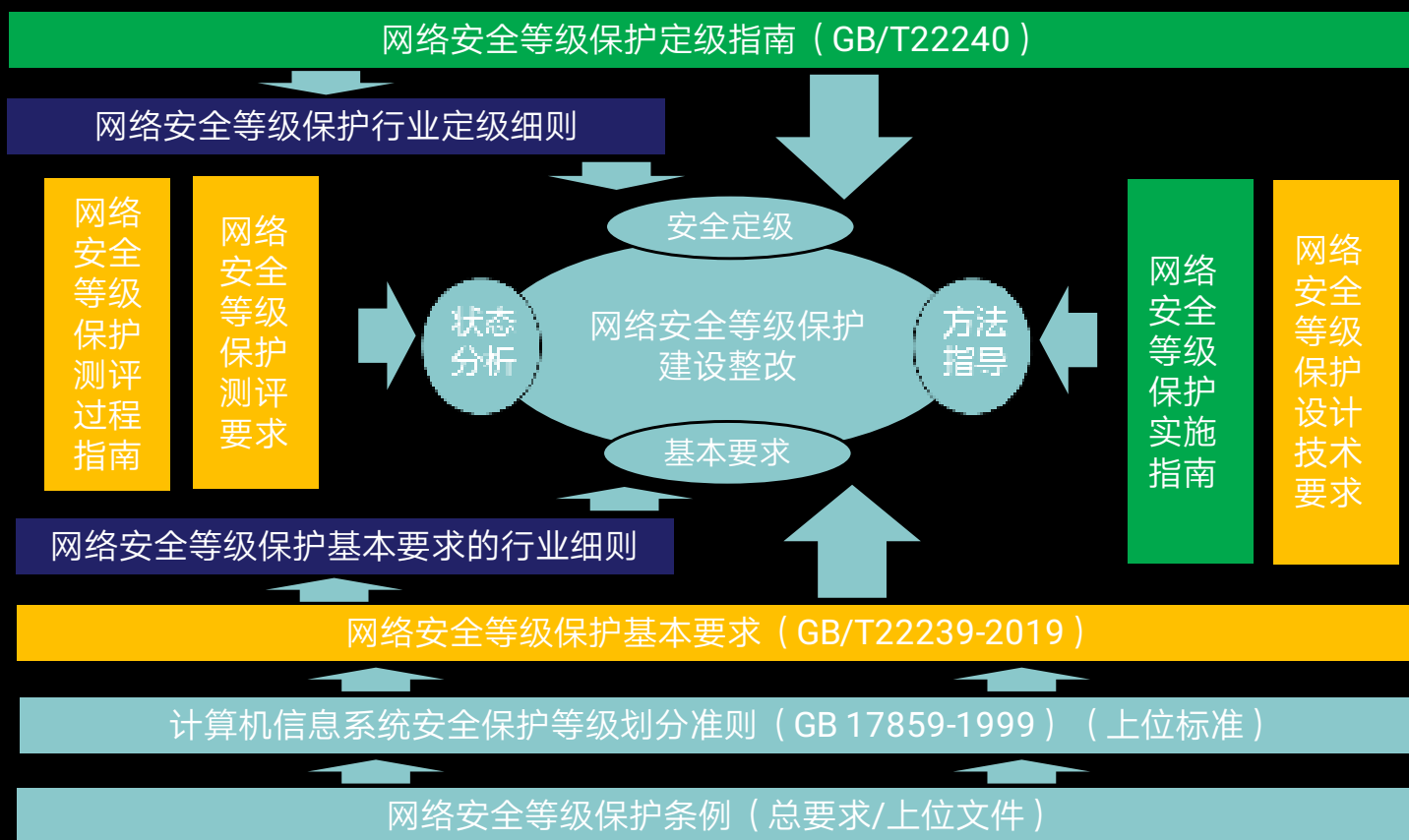
- 等保2.0是一个时代！
- 等级保护制度2.0国家标准的发布，是国家保护网络安全具有里程碑意义的一件大事，标志着网络安全等级保护制度步入新时代，对保障和促进国家信息化发展，提升国家网络安全保护能力，维护国家保护空间安全具有重要的意义。



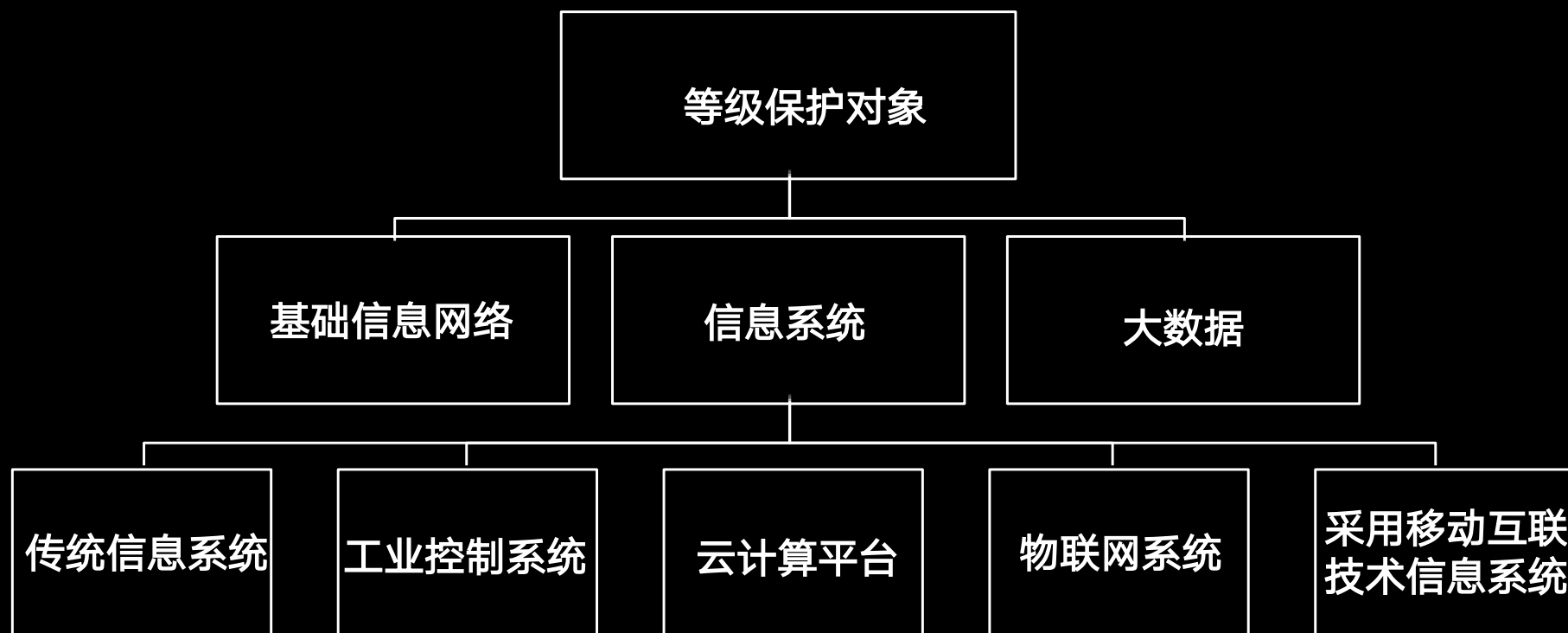
目录

- ◆ 网络安全等级保护2.0概述
- ◆ 等保2.0的特点
- ◆ 主要标准介绍
- ◆ 其他

等保2.0体系变化

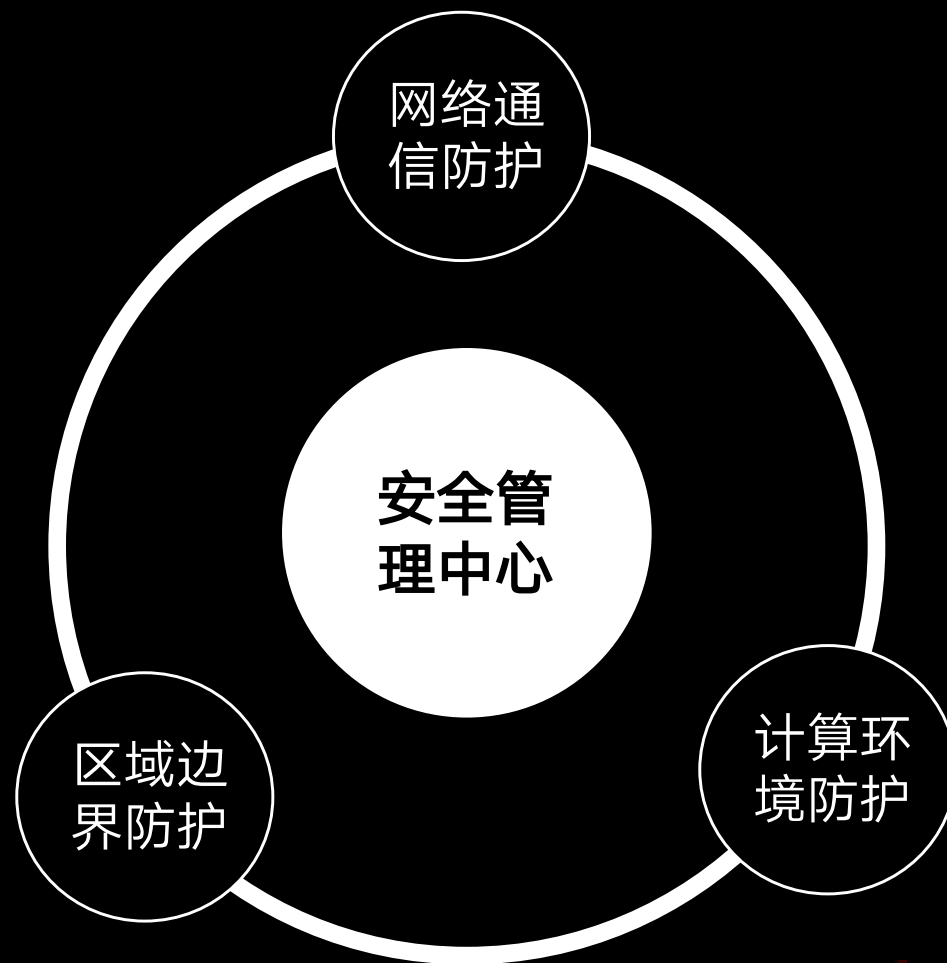


对象范围扩大



分类结构统一

- 基本要求
- 设计要求
- 测评要求



分类结构的变化（2017试用稿）

□ 结构和分类调整为：

■ 技术部分：

- 物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全；

■ 管理部分：

- 安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理

分类结构的变化（正式发布稿）

□ 技术部分：

- 安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心

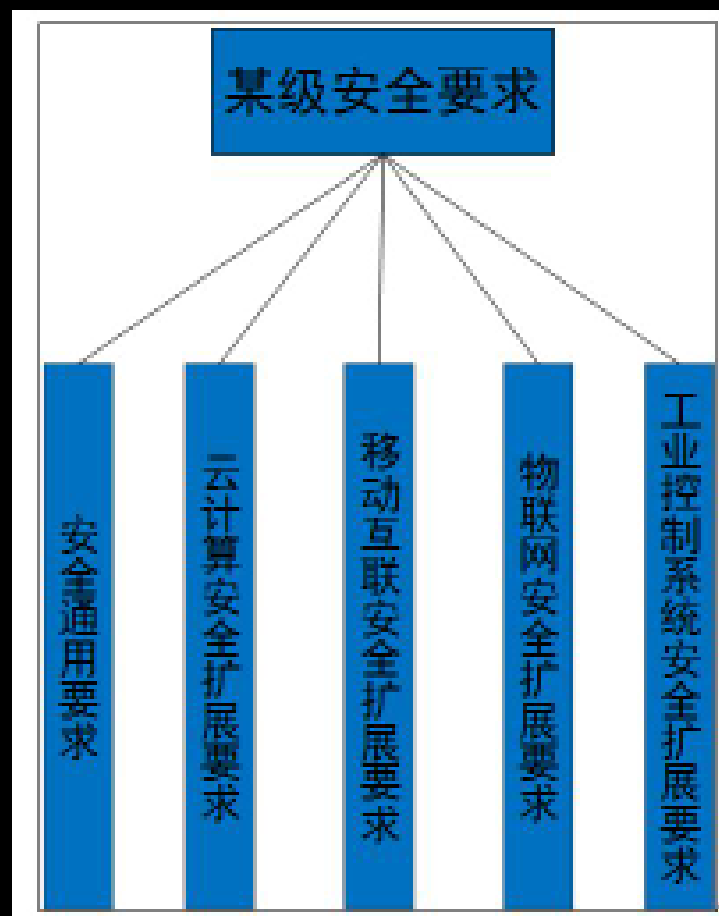
□ 管理部分：

- 安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理

安全要求的变化

- 原来：安全要求
- 改为：安全通用要求和安全扩展要求

安全通用要求是不管等级保护对象形态如何必须满足的要求，针对云计算、移动互联、物联网和工业控制系统提出了特殊要求，称为安全扩展要求。





目录

- ◆ 网络安全等级保护2.0概述
- ◆ 等保2.0的特点
- ◆ 主要标准介绍
- ◆ 其他



主要标准介绍-网络安全法

中华人民共和国主席令 第五十三号

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016年11月7日通过，现予公布，自**2017年6月1日**起施行。

中华人民共和国主席 习近平
2016年11月7日

《网络安全法》共7章79条法规，具体操作性的条款38条，主要分布在第三、四、五章。

第一章 总则	14条规定
第二章 网络安全支持与促进	6条规定
第三章 网络运行安全	19条规定
第一节 一般规定	10条规定
第二节 关键信息基础设施的运行安全	9条规定
第四章 网络信息安全	11条规定
第五章 监测预警与应急处置	8条规定
第六章 法律责任	17条规定
第七章 附则	4条规定

主要标准介绍-网络安全法

（一）管辖范围：

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，适用本法（ 第二条）

（二）管辖对象：

- 网络运营者（定义：网络的所有者、管理者和网络服务提供者）
- 关键信息基础设施的运营者
- 跨境传输者
- 网络产品或者服务的提供者



主要标准介绍-网络安全法

网络安全等级保护

国家实行网络安全等级保护制度，是安全合法的第一道门槛。

关键信息基础设施

关键信息基础设施是重中之重，要求重点保护。

个人信息保护

明确个人信息收集、使用及保护提出安全要求。

网络运营者

网络的所有者、管理者和网络服务提供者。

敏感数据存管

对个人信息和敏感数据出境提供安全要求。

安全产品认证

网络关键设备和安全设备应获得安全认证合规后才能销售和提供。

法律责任

对违反《网络安全法》的企业和组织，最高处罚金额可达100万元。



主要标准介绍-网络安全法

《网络安全法》处罚条款

处罚主体	责任方处罚	责任人处罚
网络存在较大安全风险或者发生安全事件的	整改	约谈、警告
拒不改正或者导致危害网络安全等后果的	10k-100k并整改	5k-10k
关键信息基础设施拒不改正或者导致危害网络安全等后果的	100k-100w并整改	10k-100k
设置恶意程序；对风险未立即采取补救；擅自中止产品、服务的	50k-500k并整改	10k-100k
对社会发布系统漏洞、计算机病毒、网络攻击、网络入侵等网络安全信息的	10k-100k并停业整顿	5k-50k
从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的	单位有前款行为 10w-100w且没收所得	50k-500k且五日以下拘留； 情节严重者： 10w-100w且五日以上十五日以下拘留

主要标准介绍-网络安全法

《网络安全法》监管机构

主要负责国家网络空间安全总体统筹，同时针对国家关键信息基础设施安全防护，保护对象是重中之重。



中华人民共和国国家互联网信息办公室

Cyberspace Administration of China



中华人民共和国公安部

The Ministry of Public Security of the People's Republic of China

主要负责涉及国家、经济、社会秩序、公共利益以及公民、组织合法权益等重要信息系统安全执法检查。



中华人民共和国工业和信息化部

Ministry of Industry and Information Technology of the People's Republic of China

主要负责互联网新技术、新业务、新应用的相关安全，偏向基础电信、互联网以及网上有害信息的防治领域。

主要标准介绍-网络安全等级保护条例

2018年6月27日，公安部正式发布《网络安全等级保护条例（征求意见稿）》标志着《网络安全法》第二十一条所确立的网络安全等级保护制度有了具体的实施依据与有力抓手。

主要标准介绍-网络安全等级保护条例



中华人民共和国公安部

The Ministry of Public Security of the People's Republic of China

[返回首页](#)[信息公开](#)[办事服务](#)[警民互动](#)

公安部关于《网络安全等级保护条例（征求意见稿）》公开征求意见的公告

时间：2018年06月27日 字体：【大】【中】【小】

公安部关于《网络安全等级保护条例（征求意见稿）》 公开征求意见的公告

为贯彻落实《中华人民共和国网络安全法》，深入推进实施国家网络安全等级保护制度，经广泛征求意见，反复研究修改，公安部会同有关部门起草了《网络安全等级保护条例（征求意见稿）》。为保障公众知情权和参与权，凝聚各界共识和智慧，提高立法质量，现向社会公开征求意见。

主要标准介绍-网络安全等级保护条例

相较于2007年实施的《信息安全等级保护管理办法》所确立的等级保护1.0体系，《网络安全等级保护条例》在国家支持、定级备案、密码管理等多个方面进行了更新与完善，适应了现阶段网络安全的新形势、新变化以及新技术、新应用发展的要求，标志着等级保护正式迈入**2.0**时代。

主要标准介绍-个人信息安全规范

全国信息安全标准化技术委员会制定的《信息安全技术 个人信息安全规范》（以下简称《个人信息安全规范》）于2018年5月1日正式施行。在信息时代下，为个人信息保护再次添砖加瓦

主要标准介绍-个人信息安全规范

《个人信息安全规范》旨在针对个人信息安全出现的泄露、非法收集、滥用等多个问题，规范个人信息控制者在信息的收集、保存、共享、转让等处理环节的相关行为，从而达到个人信息保护的目的。



主要标准介绍-个人信息安全规范

个人信息安全基本原则

权责一致原则

目的明确原则

选择同意原则

最少够用原则

公开透明原则

确保安全原则

主体参与原则



目录

- ◆ 网络安全等级保护2.0概述
- ◆ 等保2.0的特点
- ◆ 主要标准介绍
- ◆ 其他

主体职责



各地监管单位，对信息系统网络安全情况负有**监督、指导**的职责。要求从**技术能力**与**管理能力**双向提升，以满足在等保2.0监管过程中的检查、处置、指导、协调、统筹等工作需求。

测评机构是系统运营使用单位等保2.0建设情况的“裁判官”，必须对等保2.0涉及到的“云、大、物、移、工”等新型系统具备充分的业务能力。不断加强自身对等保2.0的贯彻理解。



主体职责

系统运营单位应当遵守法律法规、履行网络安全保护义务，保障网络安全、稳定运行。必须保质保量完成自身信息系统的等级保护建设工作，满足等保2.0下的安全合规要求。



行业组织应当加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全水平，促进行业健康发展。

面对新形势，我们还需要做

落实网络安全等级
保护制度

履行网络
运营者网
络安全保
护义务

关键信息
基础设施
认定和网
络安全保
护义务

面对新形势，我们还需要做的更多

数据本地化存储和跨境传输安全评估

个人信息和数据的保护

落实网络安全审查制度

网络传播内容的管理



THANK YOU