

电信和互联网行业 网络安全政策及监管要求



网络空间安全测评工程技术中心

白利芳

2020.3.18



中国软件评测中心

(工业和信息化部软件与集成电路促进中心)

目 录

- 01 ↪ 单位简介
- 02 ↪ 国内网络安全监管形势
- 03 ↪ 行业安全政策及监管要求
- 04 ↪ 行业落实情况及相关建议



中国软件评测中心

中国软件评测中心（工业和信息化部软件与集成电路促进中心），简称中国软件评测中心，国内权威的第三方软、硬件产品及系统质量检测、认证机构，是直属于工业和信息化部的一类科研事业单位。成立30年来秉承“专业就是实力”的宗旨，共承担10万余款软硬件产品和1万余项信息系统工程的测试任务，共测评800多个网络信息安全类项目，1300多个网络信息安全类系统。业务网络覆盖全国500多个城市，先后成立了广州、深圳、重庆、大连、上海、无锡、济宁、青岛等多个分中心，服务范围涵盖了全国31个省及直辖市。网络空间安全测评工程技术中心在武汉成立华中办事处。

通过评测、监理、认证、评估、设计等主营业务，构建基于第三方服务的科技产业链，旗下的赛迪评测、赛迪监理、赛迪认证、赛迪评估、赛迪设计等业务在业内拥有权威地位。

先后申请了40余个国家科研项目，建立了多个国家技术服务平台和重点实验室，开发了具有自主知识产权的30余种专业测试工具，获得了70余项软件著作权，具有3项专利，拥有30余项国家级管理体系认证及资质证书，并主持或参与了数十余项信息技术领域国家标准和行业标准的制定。



单位简介

CSTC 中国评测

测评、监理、认证、评估、设计5大领域，37项核心资质，17个重点实验室及国家级平台

测试/安全资质

通信网络安全服务能力评定（风险评估二级）
ISCCC信息安全服务资质认证（信息安全风险评估一级）
信息安全服务资质（安全工程类一级）
网络与信息安全信息通报机制技术支撑单位
国家网络安全等级保护测评机构
ISO/IEC 27001 信息安全管理体系认证
国家认监委检验检测机构资质认定(CMA)
中国合格评定国家认可委(CNAS)实验室认可
中国合格评定国家认可委(CNAS)检验机构认可
国家智能终端软件产品质量监督检验中心
国家机器人质量监督检验中心（北京）
GB/T 19001 质量管理体系认证
北京市软件产品登记检测机构
ITSS云服务能力评估机构
国家军工保密资格认可委员会军工一级保密资格单位
武器装备质量体系认证委员会武器装备质量体系认证
总装备部军用实验室认可
后勤军工产品检测试验机构
国防科工局武器装备科研生产许可

设计资质

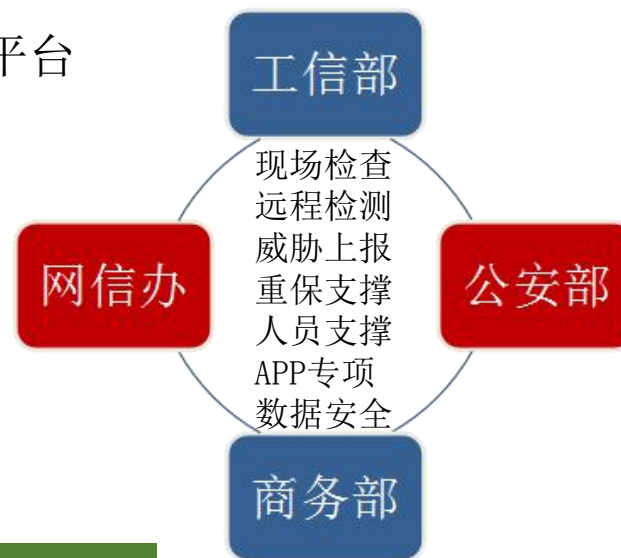
GB/T 19001质量管理体系认证
（电子系统工程）专业乙级工程设计资质

认证资质

国家认监委批准认证机构（机械设备及零部件、
数据中心能效等级、电子招标投标系统认证资
质、电信服务）
软件过程及能力成熟度评估机构
信息系统集成及服务资质评审机构
ITSS 咨询设计通用要求符合性评估机构
ITSS 运行维护标准符合性评估机构
ITSS数据中心服务能力成熟度符合性评估机构
中国机器人检测认证机构

监理资质

信息系统工程监理单位甲级资质
涉及国家秘密的计算机信息系统集成甲级资质
（工程监理）
通信建设监理企业乙级资质
军工涉密业务咨询服务安全保密条件备案资质
GB/T 19001 质量管理体系认证
GB/T 24001 环境管理体系认证
OHSAS18001 职业健康管理体系认证
ISO/IEC 20000-1 IT 服务管理体系认证
ISO/IEC 27001 信息安全管理体系认证



实验室/平台

智能制造测试验证与评价工业和信息化部重点实验室
智能网联驾驶测试与评价工业和信息化部重点实验室
机器人质量基础共性技术检测与评定工业和信息化部
重点实验室
工业控制系统安全可靠测评共性技术工业和信息化部
重点实验室
基础软件质量控制与技术评价工业和信息化部重点实
验室
工业产品质量控制和技术评价实验室
国家软件与集成电路公共服务平台——自主空间
国家云计算公共服务平台（中国测试云）
国家物联网公共服务平台
国家光伏产品公共服务平台
国家中小企业公共服务示范平台
中国信息技术服务产业平台
电子认证服务平台

国内网络安全监管形势

CSTC 中国评测



- 网络安全的国家战略地位, 直接推动网络安全监管进入新的阶段
- 多头分管、职能交叉



监管现状

- 《网安法》 第八条：国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。



监管要求——主要政策、标准

网络安全防护工作坚持积极防御、综合防范、分级保护的原则

- 《通信网络安全防护管理办法》（工信部11号令）
- 《电信和互联网用户个人信息保护规定》（工信部24号令）
- 《公共互联网网络安全威胁监测与处置办法》（工网安[2017]202号）
- YDT 1728-2008 电信网和互联网安全防护管理指南
- YDT 1729-2008 《电信网和互联网安全等级保护实施指南》
- YDT 1730-2008 《电信网和互联网安全风险评估实施指南》
- YDT 1731-2008 《电信网和互联网安全灾难备份及恢复实施指南》
- YDT XXXXXX安全防护要求
- YDT XXXXXX安全防护检测要求 （50余个专业的安全防护要求、检测要求、基线配置要求）
- YDT XXXXXX安全防护基线配置要求

具有
法律
效力

监管要求1——“三同步”要求

三同步：同步规划、同步建设、同步运行

- **《网安法》第三十三条**：建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。
- **输出“三同步”落实情况报告，并提交备案系统 (<https://www.mii-aqfh.cn/>)**
- 在对电信网和互联网及相关系统进行新建、改建、扩建时，应当同步规划和设计其安全方案，同步建设其安全保障设施，并与主体工程同时进行验收和投入运行。
- 报告内容主要体现是如何将安全防护工作和主体工程同步规划、同步建设、同步运行的。

监管要求2——定级备案

定级单位是网络单元

主要依据：《电信网和互联网安全等级保护实施指南》、11号令

□ 网元划分，识别定级对象

- 主要根据业务、服务地域、责任主体等因素来划分，原则是每个定级对象应属于同一类型的网络/系统，并由单一的责任主体负责。

□ 确定级别

- 按照定级对象遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度，根据社会影响力、规模和服务范围、所提供服务的重要性3个定级因素，由低到高分别划分五个级别。

□ 定级评审

- 电信管理机构应当组织专家对通信网络单元的分级情况进行评审；
应根据实际情况适时调整通信网络单元的划分和级别，并进行评审。



监管要求2——定级备案

线上备案

主要依据：《通信网络安全防护管理办法》（工信部11号令）

□ 备案 (<https://www.mii-aqfh.cn/>)

- 定级评审通过后三十日内，将通信网络单元的划分和定级情况按照以下规定向电信管理机构备案：

一. 基础电信业务经营者

- a. 集团公司向工信部申请办理；
- b. 各省（自治区、直辖市）子公司、分公司向当地通信管理局申请办理；

二. 增值电信业务经营者——向作出电信业务经营许可决定的电信管理机构备案；

- a. 涉外资、跨区经营的一般向工信部申请办理；
- b. 属地经营的一般向当地通信管理局申请办理；

三. 互联网域名服务提供者向工信部备案。

注：所有等级全部强制备案

监管要求3——安全风险评估

遵循等级保护原则、风评为具体方法

主要依据：《通信网络安全防护管理办法》（工信部11号令）

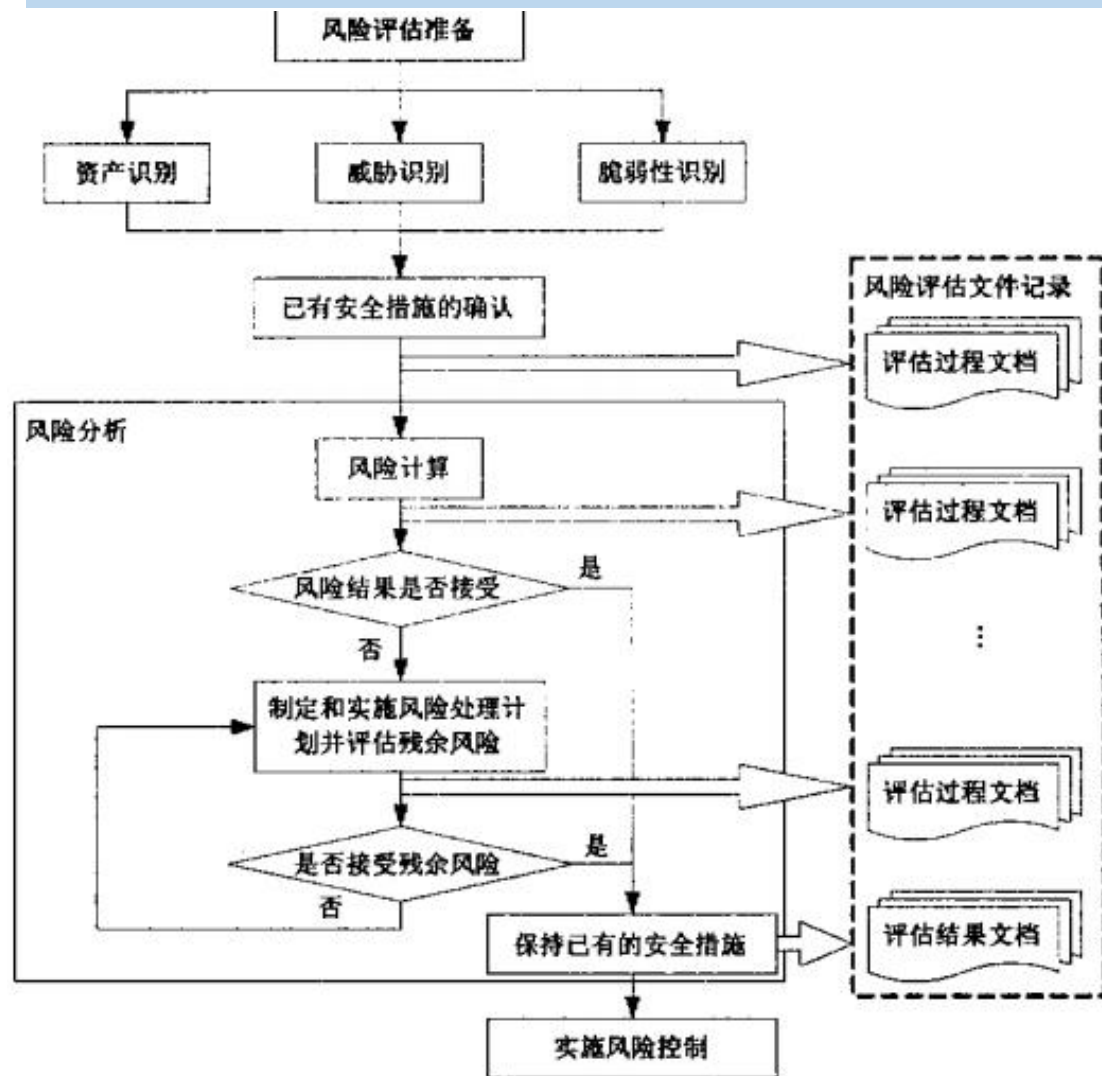
□ 具体要求：

- 三级及三级以上通信网络单元应当每年进行一次安全风险评估；
- 二级通信网络单元应当每两年进行一次安全风险评估。
- 国家重大活动举办前，通信网络单元应当按照电信管理机构的要求进行安全风险评估。
- 通信网络运行单位应当在安全风险评估结束后三十日内，将安全风险评估结果、隐患处理情况或者处理计划报送通信网络单元的备案机构。

监管要求3——安全风险评估

具体实施——自评估/专业机构评估

主要依据：《电信网和互联网安全风险评估实施指南》



识别

资产

软件、硬件、数据、服务、文档、人员等

脆弱性

技术：漏洞扫描、渗透测试、基线核查等

管理：访谈、资料查阅等

威胁

技术因素、环境因素、人为因素（恶意、非恶意）

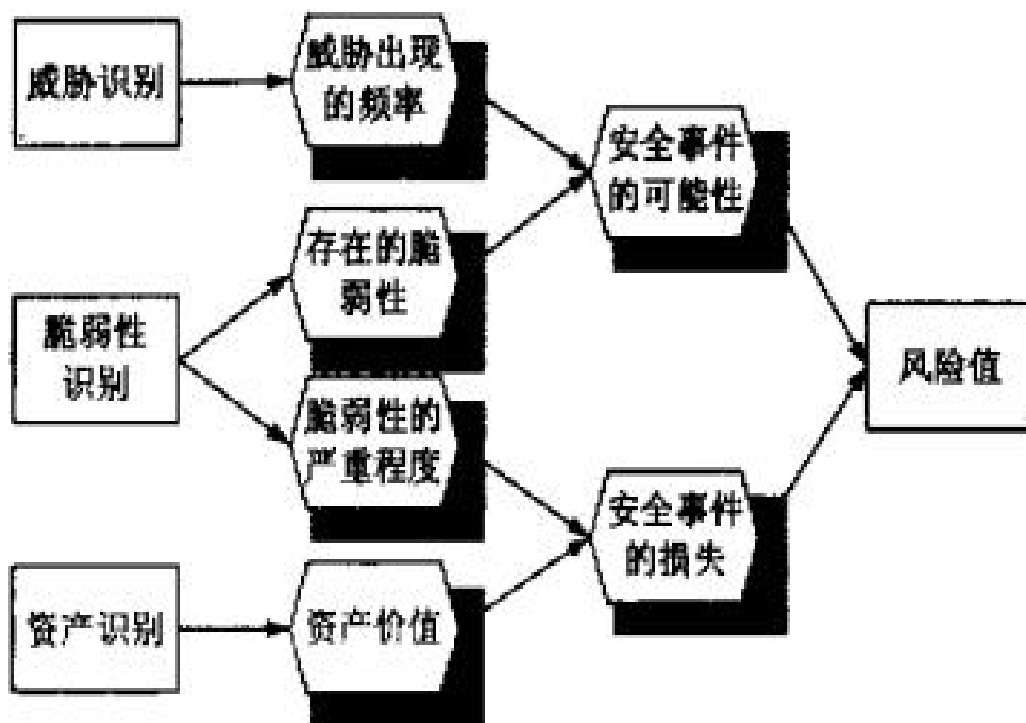
已有安全措施

有效性，核查是否应取消或替代

监管要求3——安全风险评估

具体实施——自评估/专业机构评估

主要依据：《电信网和互联网安全风险评估实施指南》



量化赋值

资产

重要程度：社会影响力、业务价值、可用性

脆弱性

严重程度：对资产的损害程度、流程度、技术实现难易程度

威胁

出现频率：经验或有关统计数据

风险

风险值：安全事件的可能性、损失程度(最后风险结果等级判定、风险处理计划/处理结果)

监管要求4——符合性评测

遵循等级保护原则、符合性评测为具体方法

主要依据：《通信网络安全防护管理办法》（工信部11号令）

□ 具体要求：

- 三级及三级以上通信网络单元应当每年进行一次符合性评测；
- 二级通信网络单元应当每两年进行一次符合性评测。
- 通信网络单元的划分和级别调整的，应当自调整完成之日起九十日内重新进行符合性评测。
- 通信网络运行单位应当在评测结束后三十日内，将通信网络单元的符合性评测结果、整改情况或者
整改计划报送通信网络单元的备案机构。

监管要求5——个人信息保护

YD/T 2781-2014 电信和互联网服务 用户个人信息保护 定义及分类
YD/T 2782-2014 电信和互联网服务 用户个人信息保护 分级指南

收集和使用规范

主要依据：《电信和互联网用户个人信息保护规定》（工信部24号令）



应制定用户个人信息收集、使用规则，并在其经营或者服务场所、网站等予以公布



未经用户同意，电信业务经营者、互联网信息服务提供者不得收集、使用用户个人信息



收集、使用用户个人信息的，应明确告知收集、使用信息的目的、方式和范围，查询、更正信息的渠道及拒绝提供信息的后果等事项



不得收集其提供服务所必需以外的用户个人信息或者将信息用于提供服务之外的目的，不得以欺骗、误导或者强迫等方式或者违反法律、行政法规以及双方的约定收集、使用信息



在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务



应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供

——具体安全保障措施、监督检查及法律责任详见《规定》

（责令限期改正、予以警告、罚款、向社会公告、刑事责任）

监管要求6——网络安全威胁监测与处置

主要依据：《公共互联网网络安全威胁监测与处置办法》（工信部网安[2017]202号）

公共互联网网络安全威胁监测与处置



应加强网络安全威胁监测与处置工作，明确责任部门、责任人和联系人，加强相关技术手段建设



发现网络安全威胁后，属于本单位自身问题的，应当立即进行处置，涉及其他主体的，应当及时将有关信息按照规定的内容要素和格式提交至工业和信息化部和相关省、自治区、直辖市通信管理局



部建立网络安全威胁信息共享平台，统一汇集、存储、分析、通报、发布；共享平台与相关单位网络安全监测平台实现对接；主管部门委托专业机构对提交的威胁信息进行认定，并提出处置建议



主管部门对专业机构的认定和处置意见进行审查后，可对网络安全威胁采取处置措施，详见《办法》（工网安[2017]202号）。不服的，有权在10个工作日内向做出处置决定的主管部门进行申诉



电信主管部门的处置通知应当通过书面或可验证来源的电子方式等形式送达相关单位，紧急情况下，可先电话通知，后补书面通知



应为电信主管部门依法查询IP地址归属、域名注册等信息提供技术支持和协助，并按通知和时限要求采取相应处置措施，反馈处置结果。负责网络安全威胁认定的专业机构应当对相关处置情况进行验证（约谈或给予警告、罚款等行政处罚）

监管要求——其他

主要依据：《通信网络安全防护管理办法》（工信部11号令）

□ 具体要求：

- 安全保障设施的新建、改建、扩建费用，应当纳入本单位建设项目概算。
- 应对通信网络单元的重要线路、设备、系统和数据等进行备份。
- 应组织演练，检验通信网络安全防护措施的有效性。
- 应参加电信管理机构组织开展的演练。
- 应建设和运行通信网络安全监测系统，对本单位通信网络的安全状况进行监测。

监管方式——现场网络安全检查

现场网络安全检查



定级备案及“三同步”落实情况

是否定级备案，查阅定级备案报告、“三同步”落实情况报告等



法律法规落实情况（网安法、11号、24号令）

安全风险评估、符合性评测、个人信息保护等是否按要求开展



基线核查

基线配置是否按要求开展，人工核查或工具基线扫描



符合性评测

根据对应网元的符合性评测表逐条测试、核查



技术检测

漏洞扫描、人工渗透

- 频率：年度、分批次双随机
- 检查机构：部里或属地管局授权委托

中华人民共和国工业和信息化部

工网安[]号

网络安全检查通知书

有限公司：
为做好党的十九大网络安全保障工作，按照重大活动网络安全保障工作要求，根据《通信网络安全防护管理办法》（工业和信息化部令第11号）、《电信和互联网用户个人信息保护规定》（工业和信息化部令第24号），我局决定组织开展2017年网络安全检查工作。现委托中国软件评测中心于2017年7月7日至7月30日对 进行网络安全检查。检查网络和系统运行单位网络安全法律法规和标准落实情况，网络与系统

监管方式——远程安全监测、检测、专项检查

远程安全监测

- **监管对象：**暴露在互联网上的网元
- **报送方式：**主要报送至网络安全威胁信息共享平台
- **参与单位：**与威胁共享平台实现对接的相关单位可以上报威胁信息、由主管单位委托的专业机构进行认定

远程安全检测

- **监管对象：**暴露在互联网上的网元
- **报送方式：**定期报送部里
- **检测机构：**部里授权委托专业机构

专项检查

- APP安全专项、数据安全专项、个人信息安全专项等
- **检查机构：**部里委托专业机构

中华人民共和国工业和信息化部

工网安[2017]202号

关于委托开展远程技术检测的函

中国软件评测中心：

为及时发现并消除网络安全隐患，切实提升电信和互联网行业网络安全防护水平，依据《中华人民共和国网络安全法》、《通信网络安全防护管理办法》（工业和信息化部令第11号）、《公共互联网网络安全威胁监测与处置办法》（工信部网安〔2017〕202号）等相关规定，委托你单位对基础电信企业、互联网企业、域名注册管理和服务机构等相关单位的业务系统、工业互联网平台和移动应用等开展远程技术检测。

一、工作目标

法律责任

- 11号令明确规定，通信网络运行单位应配合电信管理机构及其委托的专业机构开展检查活动，对于检查中发现的重大网络安全隐患，应当及时整改。（定级备案、风评、符合性评测...）
- 违反11号令相应条款规定的，由电信管理机构依据职权责令改正；拒不改正的，给予警告，并处五千元以上三万元以下的罚款。（年报不通过、约谈、公开通报、产品下架等）



行业等保VS等保2.0

对比项目	行业等保	等保2.0
适用范围	基础电信业务经营者和增值电信业务经营者管理和运行的网络/系统	涉网企业或组织运营、使用的系统（行业内的在各自职责内开展）
政策依据	《通信网络安全防护管理办法》	《信息安全等级保护管理办法》
定级要求	五级，第三级又分为第3.1级和第3.2级	五级
备案要求	所有等级强制备案；线上备案；备案机构为工信部或省管局；提交材料	二级及以上强制备案；线下备案；备案机构为公安部或属地公安机构；提交材料
实施方法	主要为安全风险评估、符合性评测	主要为等级保护测评
等级要求	二级每两年一次；三级及以上每年一次	三级以上每年一次
监管方式	年度现场检查、远程检测和监测、专项检查	年度抽查、专项检查、测评机构能力验证
测评机构	专业机构（具备行业相应安全资质或主管部门委托）	等保办推荐测评机构
法律责任	责令改正、警告、罚款（年报不通过、约谈、通报、考核问责等）	限期改正；逾期不改正的，给予警告，并向其上级主管部门通报情况

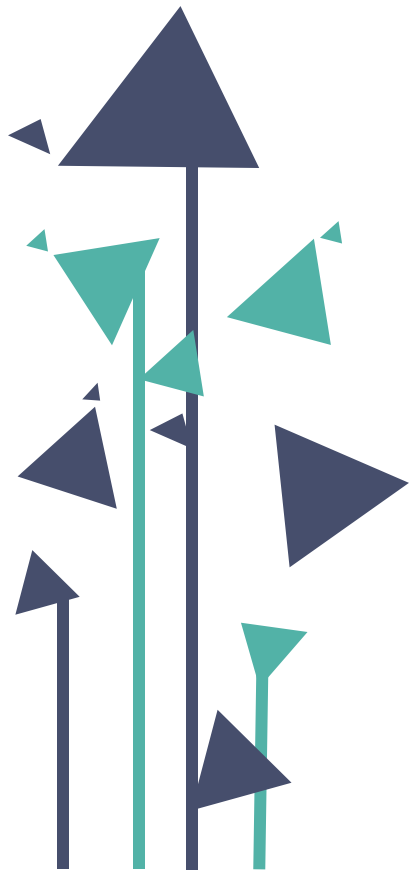
行业落实情况

□ 监管要求认识不到位

- 监管要求不了解，甚至混淆
- 对主管部门的监管有抵触情绪、不理解

□ 执行力度参差不齐

- 整体上基础电信企业较好，增值业务企业大多未按要求落实，如定级备案、风险评估和符合性评测等工作的开展，如何开展
- 重技术轻管理、尚有企业安全意识薄弱，如未配备专门的安全岗位及安全管理人员



相关建议

□ 意识提升

- 宣贯教育、安全培训、自我学习提升等

□ 落实到位

- 实行安全责任制，紧盯行业监管要求，抓好技术和管理具体落实
- 加强与主管部门必要的沟通交流

□ 积极参与

- 年度部网络安全试点示范项目
- 网络安全宣传周



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



工业和信息化部

新闻动态

信息公开

政务服务

公众参与

工信数据

专题专栏

首页 > 信息公开 > 政策文件 > 文件发布 > 其他 > 正文

分享:

发文机关：办公厅

标 题：工业和信息化部办公厅关于公布网络安全技术应用试点示范项目名单的通知

发文字号：工信厅网安函〔2019〕116号

成文日期：2019-05-15

发布日期：2019-06-04

文章来源：网络安全管理局

分 类：网络安全管理

工业和信息化部办公厅关于公布网络安全技术应用试点示范项目名单的通知

工信厅网安函〔2019〕116号

各省、自治区、直辖市及计划单列市工业和信息化主管部门，各省、自治区、直辖市通信管理局，部属相关单位，相关中央企业，各有关单位：

国家层面

- **法律**——如《网安法》《密码法》.....**主席令**
- **法规**——XX条例、XX办法，如《中华人民共和国电信条例》国务院291号令、《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、《互联网信息服务管理办法》国务院292号令、《关键信息基础设施安全保护条例》(征).....**国务院令**
- **国标**——XX要求、XX检测要求、XX指南.....**GB/**

行业层面

- **法规**——如《电信业务经营许可管理办法》（工信部5号令），《通信网络安全防护管理办法》（工信部11号令）.....**部令**
- ——《公共互联网网络安全威胁监测与处置办法》(工网安[2017]202号).....**局文/函**
- **行标**——XX要求、XX检测要求、XX指南.....



THANKS



bailifang@cstc.org.cn

CSTC
中国评测

—— 专业就是实力 ——