



公开征求对《关于促进网络安全产业发展的指导意见（征求意见稿）》的意见

发布时间：2019-09-27 来源：网络安全管理局

分享:    

为贯彻落实《中华人民共和国网络安全法》，积极发展网络安全产业，工业和信息化部会同有关部门起草了《关于促进网络安全产业发展的指导意见（征求意见稿）》（见附件），现面向社会公开征求意见。如有意见或建议，请于2019年10月11日前反馈。

联系电话：010-66022774

传 真：010-66022774

邮 箱：wangmeifang@miit.gov.cn

附件：关于促进网络安全产业发展的指导意见（征求意见稿）.docx

工业和信息化部
2019年9月27日

关于促进网络安全产业发展的指导意见

（征求意见稿）

没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。当前，各种形式的网络攻击、黑客入侵、恶意代码、安全漏洞层出不穷，对关键信息基础设施安全、数据安全、个人信息安全构成严重威胁。网络安全的本质是技术对抗，保障网络安全离不开网络安全技术和产业的有力支撑。近年来，我国网络安全产业规模快速增长、产品体系相对完善、创新能力逐步增强、发展环境明显优化，但与网络安全保障要求相比，还存在核心技术欠缺、产业规模较小、市场需求不足、产业协同不够等问题。为积极发展网络安全产业，提升网络安全技术支撑保障水平，制定本指导意见。

一、总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平总书记关于网络安全的系列重要讲话精神，坚持新发展理念，树立正确的网络安全观，贯彻落实《网络安全法》，以服务国家网络空间安全战略需求为导向，主动应对互联网、

应对5G、工业互联网、下一代互联网、物联网等新技术新应用带来的新挑战，坚持市场主导、政府引导，着力突破关键技术、构建产业生态、优化发展环境，推动我国网络安全产业高质量发展，为维护国家网络空间安全、保障网络强国建设提供有力的产业支撑。

（二）基本原则

创新驱动。大力推动技术、产品创新，突破技术瓶颈，着力提升网络安全核心技术能力。创新网络安全服务模式，提升网络安全专业化服务水平，实现产业发展逐步由产品主导向服务主导转变。

协同发展。充分调动各方力量，加强产学研合作，鼓励技术成果转化，推动强强联合、协同攻关，构建多方参与、优势互补、融合发展的产业生态体系。推动产融合作，引导社会资本参与网络安全产业发展。

需求引领。推动各行业各领域持续加大网络安全投入，坚持问题导向，加强供需对接，促使产业更好满足金融、能源、通信、交通、电子政务等重点领域网络安全需求。

开放合作。推动网络安全产业国际交流合作，学习借鉴国外产业发展模式，促进技术、人才交流和信息共享，积极参与“一带一路”建设，提升产业国际竞争力。

（三）发展目标

网络安全技术创新能力显著增强，网络安全产品和服务体系更加健全，网络安全职业人才队伍日益壮大，政产学研用资协同发展的网络安全产业格局不断巩固，产业发展环境更加优化，网络安全产业维护国家网络空间安全、保障网络强国建设的支撑能力大幅提升。到 2025 年，培育形成一批年营收超过 20 亿的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，网络安全产业规模超过 2000 亿。

二、主要任务

（一）着力突破网络安全关键技术

以构建先进完备的网络安全产品体系为目标，聚焦网络安全事前防护、事中监测、事后处置、调查取证等环节需要，大力推动资产识别、漏洞挖掘、病毒查杀、边界防护、入侵防御、源码检测、数据保护、追踪溯源等网络安全产品演进升级，着力提升隐患排查、态势感知、应急处置和追踪溯源能力。加强 5G、下一代互联网、工业互联网、物联网、车联网等新兴领域网络安全威胁和风险分析，大力推动相关场景下的网络安全技术产品研发。支持云计算、大数据、人工智能、量子计算等技术在网络安全领域的应用，着力提升威胁情报分析、智能监测预警、加密通信等网络安全防御能力。积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构，推动网络安全理论和技术创新。

（二）积极创新网络安全服务模式

针对网络安全专业性强、技术演进快、应用难度大的特点，倡导“安全即服务”的理念，鼓励网络安全企业由提供安全产品向提供安全服务和解决方案转变。支持专业机构和企业开展网络安全规划咨询、威胁情报、风险评估、检测认证、安全集成、应急响应等安全服务，规范漏洞扫描、披露等活动。支持合法设立的认证机构依法开展网络安全认证。大力发展基于云模式的网络安全公共服务平台，提供远程实时在线的漏洞发现、网站防护、抗拒绝服务攻击、域名安全等服务。鼓励基础电信企业和云服务提供商发挥网络资源优势，面向客户提供网络安全监测预警、攻击防护、应急保障等增值服务。鼓励发展面向智慧城市建设和电子政务等领域的网络安全一体化运营外包服务。探索开展网络安全保险服务。

（三）合力打造网络安全产业生态

支持龙头骨干企业整合网络安全创新链、产业链、价值链，建立开放性网络安全技术研发、标准验证、成果转化平台，畅通创新能力对接转化渠道，实现大中小企业之间多维度、多触点的创新能力共享、创新成果转化和品牌协同。着力培育主营业务突出、竞争能力强、成长性好的网络安全中小企业，鼓励以专业化分工、服务外包、共享研发等方式与大企业相互合作，形成协同共赢格局。充分调动各类园区、企业、科研院所、金融机构等主体的积极性和主动性，鼓励

集聚、集约、关联、成链、合作发展。培育建设一批网络安全技术、产品协同创新平台和实验室，开展共性重要问题和市场亟需方向的联合研究，充分发挥科技支撑引领作用，推动产业共性技术研发和推广应用，引导创新资源集聚。鼓励企业、研究机构、高校、行业组织等积极参与制定网络安全相关国家标准、行业标准。

（四）大力推广网络安全技术应用

充分发挥党政机关和相关行业主管部门作用，推动先进适用网络安全技术产品和服务在金融、能源、通信、交通、电子政务等重要领域的部署应用。加强工业互联网、车联网、物联网安全管理，督促指导相关企业采取必要的网络安全技术措施。大力促进商用密码技术在网络安全防护中的应用。财政投资的信息化项目应当同步配套建设网络安全技术设施，并单独开展安全验收。加大对网络安全技术应用试点示范项目的支持推广力度，鼓励示范企业将解决方案转化为标准指南并开展专题宣讲。鼓励开展网络安全技术论坛和产品服务展示活动。

（五）加快构建网络安全基础设施

推动相关行业主管部门、地方政府建设本行业、本地区网络安全态势感知平台，着力提升支撑网络安全管理、应对有组织高强度攻击的能力。鼓励重点行业、骨干企业建设漏洞库、病毒库等网络安全基础资源库，促进相关主体之间的

信息共享。统筹建设国家网络安全信息共享平台和应急指挥平台，实现跨企业、跨行业、跨地区信息共享和协调联动。重点围绕工业互联网、车联网、物联网新型应用场景，建设网络安全测试验证、培训演练、设备安全检测等共性基础平台。支持构建基于商用密码、指纹识别、人脸识别等技术的网络身份认证体系。

三、保障措施

（一）加强组织领导

各地相关部门要从网络强国战略高度充分认识发展网络安全产业的重要意义，加强组织领导和统筹谋划，强化部门合作，共同营造有利于网络安全产业发展的良好环境。深入贯彻落实《网络安全法》，加快制定配套法规政策，加大网络安全监管力度，督促网络运营者落实网络安全技术措施，带动网络安全市场需求。

（二）加大政策支持力度

中央网信办指导支持国家网络安全人才与创新基地建设，会同相关部委推动网络关键设备和网络安全专用产品认证和安全检测结果互认，避免重复认证、检测。工信部推动国家网络安全产业园区建设，建立网络安全产业运行监测体系，组织开展网络安全技术应用试点示范，指导举办中国网络安全产业高峰论坛。国家发展改革委加强网络安全领域规划、政策研究制定。中央财政统筹利用中国互联网投资基金

等现有渠道，引导支持网络安全产业发展。各地可结合本地实际情况，在财政、人才引进、要素保障等方面研究制定有针对性的产业扶持政策。

（三）健全人才培养体系

推动高校设立网络空间安全学院或网络安全相关专业，加强一流网络安全学院和网络安全师资队伍建设。加强网络安全职业教育和技能培训，培养更多实用技能型人才。推动校企对接，支持设立网络安全联合实验室。鼓励举办高水平网络安全技能竞赛，健全人才发现选拔机制。支持职业技能鉴定机构、行业协会等开展网络安全人员技能鉴定和能力评定工作。

（四）推进国际交流合作

利用各种多边、双边对话机制或活动平台，加强网络安全技术、产业务实合作与交流。鼓励有实力的网络安全企业设立海外研发中心和联合实验室，引进海外高端人才和先进技术。鼓励参加和举办有影响力的网络安全国际论坛和展会，积极参与网络安全国际标准制定和协调。推动相关地方发挥区位优势，打造国际、区域性网络安全技术、产业、人才交流平台。

扫一扫在手机打开当前页



[【打印】](#) [【关闭】](#)



中国政府网 中央国家机关举报网站 网站地图

主办单位：中华人民共和国工业和信息化部 地址：中国北京西长安街13号 邮编：100804

版权所有：中华人民共和国工业和信息化部 网站标识码：bm07000001 京ICP备 04000001号



京公网安备 11040102700068号