附　件

网络安全产业高质量发展三年行动计划
(2021-2023 年)

（征求意见稿）

网络安全产业作为新兴数字产业，是维护国家网络空间安全和发展利益的网络安全技术、产品生产和服务活动，是建设制造强国和网络强国的基础保障。近年来，我国网络安全产业取得积极进展，特别是随着 5G、大数据、人工智能、车联网、工业互联网、物联网等新技术新业务新模式快速发展，网络安全、数据安全等技术、产品和服务蓬勃发展。为深入贯彻落实习近平总书记关于网络强国的重要思想，落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》，加快建设创新能力强、产业结构优、供给质量高、需求释放足、产融合作深、人才队伍专的健康有序产业发展生态，推动网络安全产业实现技术先进、产业发达的高质量发展目标，不断提升国家网络安全保障能力，制定本行动计划。

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，全面贯彻

党的十九大和十九届二中、三中、四中、五中全会精神，立足新发展阶段、贯彻新发展理念、构建新发展格局，统筹发展和安全，积极把握数字产业化和产业数字化发展机遇，加快推进供给侧结构性改革，以推动网络安全产业高质量发展为目标，以有效需求引领高质量供给为主线，充分激发技术创新活力，充分发挥各类资本支持作用，加强多层次人才支撑保障，促进创新链、产业链、价值链的协同发展，培育健康有序的产业生态，为制造强国和网络强国建设奠定坚实基础。

（二）基本原则

创新驱动，夯实基础。加强基础性、通用性、前瞻性安全技术研究，加快关键核心技术攻关，激发企业创新动力，有效推进技术成果转化，强化产业基础能力，提升产业链水平。

需求牵引，供给转型。推动重点行业加大网络安全投入，以有效需求牵引供给。引导网络安全产品向服务化、高级化转变，以高质量供给创造高层次需求。

深度融合，协同推进。坚持网络安全教育、技术、产业融合发展，强化产学研用资深度合作，支持创新联合体建设，加大资本助力作用，突出协同推进实效。

市场主导，政府引导。发挥各类市场主体作用，鼓励差异化发展和竞争。更好发挥政府规划引导、政策支持、标准制定、市场监管等作用，督促企业落实网络安全和数据安全主体责任，营造良好发展环境。

（三）发展目标

到2023年，网络安全技术创新能力明显提高，产品和服务水平不断提升，经济社会网络安全需求加快释放，产融合作精准高效，网络安全人才队伍日益壮大，产业基础能力和综合实力持续增强，产业结构布局更加优化，产业发展生态健康有序。

——**产业规模。**网络安全产业规模超过2500亿元，年复合增长率超过15%。

——**技术创新。**一批网络安全关键核心技术实现突破，达到先进水平。新兴技术与网络安全融合创新明显加快，网络安全产品、服务创新能力进一步增强。

——**企业发展。**一批质量品牌、经营效益优势明显的具有网络安全生态引领能力的领航企业初步形成，一批面向车联网、工业互联网、物联网、智慧城市等新赛道的“专精特新”中小企业群体迅速成长，网络安全产品、服务、解决方案单项冠军企业数量逐步壮大。

——**需求释放。**电信等重点行业网络安全投入占信息化投入比例达10%。重点行业领域安全应用全面提速，中小企业网络安全能力明显提升，关键行业基础设施网络安全防护水平不断提高。

——**人才培养。**建成一批网络安全人才实训基地、公共服务平台和实训靶场，创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人

才规模质量不断提高。

——**生态培育。**产融对接更加精准高效，资本赋能作用持续加大。网络安全产业结构进一步优化，产业聚集效应显著增强。以产品服务能力为导向的健康市场秩序不断完善，大中小企业融通发展的产业格局基本形成。

二、重点任务

（一）产业供给强化行动

1.加快传统安全产品升级。进一步提高入侵检测系统、高级威胁检测、网络审计、主机和终端安全、内容安全等传统检测类产品性能，优化规则提取算法，提高安全检测质量。推动防火墙、抗拒绝服务系统、安全网关等传统防护类产品安全能力集约化发展。推动安全运营平台、网络流量分析系统、威胁信息分析与溯源系统等传统分析类产品向智能化发展，提升大数据、人工智能、密码技术在安全领域的应用水平。

2.加强重点领域网络安全供给。针对 5G、云计算、人工智能等新兴技术领域，加速推动原生安全、智能编排、内生安全、动态访问控制、可信计算等技术产品研发和推广落地。针对工业互联网，强化大流量安全分析、漏洞挖掘与管理、数据融合分析、协议标识解析等能力。针对车联网和物联网，推动内生结合的轻量级终端安全产品或中间件，以及通信安全、身份认证、平台安全等防护方案应用。推动联邦学习、多方安全技术、隐私计算、密态计算、安全检索、多阈协同追踪等数据安全技

术研究应用。

3.强化数据安全技术研究与应用。针对数据防泄露、防篡改、防窃取等传统数据安全保障需求，进一步优化数据安全管理、分类分级安全防护等产品功能和性能，提升数据安全智能防护和管理水平。针对数据安全监管需求，进一步强化监测预警和应急处置技术研究，提升智能风险分析、威胁预警和自动化事件处置能力。针对数据安全共享需求，大力推进安全多方计算、联邦学习、可信计算等技术的研究攻关和部署应用，促进数据要素安全有序流动。

4.创新安全服务模式。加强安全企业技术产品的云化能力，推动云化安全产品应用，鼓励综合实力强的安全企业发展弹性、灵活的云模式网络安全服务。发展集约化安全服务，鼓励企业提供集防火墙、用户身份认证、数据安全、应用安全等一揽子整体解决方案。支持开展威胁管理、检测响应等安全托管和咨询服务。发展地区级、城市级、行业级安全运营服务，提高运营自动化、流程化、工具化水平。鼓励基础电信企业、大型云服务提供商，并充分发挥网络和基础资源优势，输出安全服务能力，同时升级改造基础设施，支持安全企业嵌入安全服务能力。

5.发展创新安全技术。推动网络安全架构向内生、自适应发展，加快开展基于开发安全运营、主动免疫、零信任等框架的网络安全体系研发。加快发展动态边界防护技术，鼓励企业深

化微隔离、软件定义边界、安全访问服务边缘框架等技术产品应用。积极发展智能检测响应技术，提升用户实体行为分析、安全编排与自动化响应、扩展检测与响应等技术应用水平。推动发展主动安全防御技术，推进欺骗防御、威胁狩猎、拟态防御等技术产品落地。加速应用基于区块链的防护技术，推进多方认证、可信数据共享等技术产品发展。加强卫星互联网、量子通信等领域安全技术攻关。

6.加强共性基础支撑。持续建设高质量威胁信息、漏洞、恶意代码、恶意地址、攻击行为特征等网络安全基础知识库，强化网络安全知识支撑能力。加快发展恶意代码检测、高级威胁监测分析、信息处理、逆向分析、漏洞分析、密码安全性分析等底层引擎和工具，提升网络安全知识使用水平。加快发展源代码分析、组件成分分析等软件供应链安全工具，提升网络安全产品安全开发水平。积极推进网络靶场技术研究，建设结合虚拟环境和真实设备的安全孪生试验床，提升网络安全技术产品测试验证能力。

专栏 1　面向新设施新要素的安全技术与产品提升工程
5G 安全。针对 5G 核心网、边缘计算平台等 5G 网络基础设施，推进安全编排与自动化响应、深度流量分析、威胁狩猎、信令安全等产品应用，推动云边协同安全能力建设。针对网络切片、网络功能虚拟化等技术特点，推动容器安全、微隔离等虚拟化安全防护产品及 5G 空口和信令防护检测等安全产品部署应用，提升 5G 内生安全能力和 5G 网络威胁的感知能力。针对 5G 虚拟专网、5G 共建共享等网络建设模式，积极

推进安全资源池、零信任安全架构、资产识别等安全解决方案应用，构建按需供给的安全能力。

云安全。面向多云、云原生、边缘云、分布式云等新型云计算架构，发展多云身份管理、云安全管理平台、云安全配置管理、云原生安全、云灾备等技术产品，推动云架构安全发展。面向云环境中云服务器、虚拟主机、网络等基础资源，加强基础信息采集水平，提升能够面向双栈（IPv4、IPv6）的流量可视化、微隔离、软件定义边界、云工作负载保护等安全产品能力，保障云上资源安全可靠。面向云上业务、应用等服务，提升安全访问服务边缘模型、云 Web 应用防火墙、云上数据保护等安全产品效能，保障云上业务安全运行。

人工智能安全。构建人工智能安全威胁分类体系，面向人工智能系统的生命周期，建立人工智能威胁模型，制定面向人工智能系统安全性检测与评估标准体系。研究人工智能系统可解释性、隐私性等安全要素，突破人工智能模型攻击与防御关键技术，设计实现人工智能系统自动攻防平台，构建人工智能安全靶场。

数据安全。优化数据安全管理技术，提升数据识别、分类分级、质量管控、血缘分析等基础性技术产品准确性和智能水平，提升质量管控、血缘分析技术能力，准确掌握数据资源情况，做到数据可视、可管、可控。完善数据应用安全防护技术，推进数据脱敏、数据防泄漏、数据加密、数据备份恢复、细粒度访问控制等技术产品升级，保障数据应用安全可控。强化数据安全监测预警和应急处置技术，提高对终端、网络、云以及跨境等场景中数据流动和异常行为监测的广度、深度和准确性，提升事件处置智能化和自动化水平。突破数据共享安全保障技术，推动安全多方计算、联邦学习、可信计算、同态加密、差分隐私、区块链、数据水印等隐私保护和流向溯源技术实用化部署和普及应用，推动国产商用密码应用，促进数据要素安全有序流动。

（二）安全需求牵引行动

7.推动电信和互联网行业网络安全能力升级。指导电信、互联网等重点行业企业加大网络安全投入，推进网络安全与信息化同步规划、同步建设和同步使用，健全网络安全管理和技术保障体系。深入开展网络安全资产测绘、监测预警、检测评估、信息共享，健全基于网络侧的木马病毒、移动恶意程序和高级威胁行为等异常行为安全监测与处置手段。强化电信、互联网行业网络安全风险评估和应急演练，增强网络安全威胁防范、隐患处理和应急处置能力，持续提升安全防护体系成熟度水平。加强数据全生命周期安全保护，实施分类分级管理，开展数据安全风险评估，提高个人数据、重要数据安全保护水平，保障人民群众的生命财产安全和个人隐私安全。

8.加快新兴融合领域安全应用。全面推动工业互联网企业网络安全分类分级落地实施，面向原材料、装备制造、消费品、电子信息等行业，针对联网工业企业、平台企业、标识解析企业等加强网络安全分级防护体系建设。面向车联网安全，鼓励整车企业提升汽车、网络关键设备及云平台的安全防护与检测能力，强化路侧联网设施安全，推动车联网示范区、先导区和测试场安全解决方案的测试验证和示范应用。实施物联网基础安全“百企千款”产品培育行动，面向物联网终端、网关、平台等物联网关键环节，开展物联网安全检测、异常处置和公共服务，打造“物联网安心产品”。

9.推动关键行业基础设施强化网络安全建设。推动能源、金融、交通、水利、卫生医疗、教育等行业领域加强资产识别、设备防护、边界防护、身份认证、数据安全、应用安全等技术手段建设，提升重要系统、关键节点及数据的安全防护能力。支持建立态势感知、通报预警、应急响应、安全运营等安全机制及纵深防护体系，不断提高风险防范和应急处置能力。推进零信任、人工智能等技术应用，提升防护体系效能。

10.推进中小企业加强网络安全能力建设。实施中小企业“安全上云”专项行动，建设网络安全运营服务中心，面向中小企业提供高质量、低成本、集约化的网络安全产品和服务。引导中小企业通过网络安全产品服务一站式购买、租赁、订阅、托管、云端交付等方式，灵活部署网络安全产品和解决方案。支持开展多元化网络安全意识宣贯和技能培训，不断提升中小企业网络安全防护意识和能力。

专栏 2　面向数字化新场景新业务的安全能力建设工程
车联网安全。强化车联网安全能力建设，针对网联汽车及其网络关键设备，推进轻量化身份认证、车载安全网关、车载防火墙、入侵检测等关键技术及产品应用，强化纵深防御技术能力建设。针对 V2X 通信，推进基于 PKI 的安全认证与审计技术，加快车联网身份认证和安全信任体系建设。针对车联网平台及应用，建设安全运营中心，推进一体化云安全防护、数据合规保护与安全检测、监测和应急处置等技术产品落地。推动网络安全技术在 OTA 升级、远程监控、自动驾驶、车路协同等重点场景的应用部署。 **工业互联网和工控安全。**面向工业互联网全业务流程，围绕设备、

控制、网络、标识、平台、数据安全防护需求，加快工业主机快照回滚、控制系统漏洞挖掘、控制系统内生安全等工控安全技术攻关，突破协议逆向分析、轻量级加密认证、大流量安全分析、工业网络安全威胁信息共享分析等工业互联网安全技术攻关。强化工业级防护设备、海量联网设备可信接入、平台安全、标识解析安全管理、工业数据全生命周期保护等安全产品推广应用，提升工业互联网场景化安全防护能力。

物联网安全。积极推进智慧能源、智慧农业、智能家居、智能穿戴设备等物联网场景网络安全应用，鼓励企业研制适应异构物联网场景下的端到端安全防护解决方案。针对物联网平台，发展基于安全传输、异常行为分析、可信身份、威胁分析、数据防泄漏等技术的平台安全类产品。针对物联网设备可信接入网关，加快发展身份识别、协议解析和安全检测分析技术，鼓励企业将更多安全能力集成至网关。针对物联网终端，加强物联网设备及固件的漏洞挖掘，研制集接口防护、安全认证、应用安全、敏感数据保护等于一体的嵌入式集约化安全产品，打造安心物联网。

智慧城市安全。适配智慧城市政务、交通、能源、制造、教育、医疗等业务场景，构建“一脑，三云”的网络安全防御能力集群，加强异构安全能力联动水平，打造动态安全防御体系。鼓励打造智慧城市安全大脑，建设网络安全“智能云”，搭建全景安全知识库、网络安全监测分析引擎及大数据中心，以全局视角提升网络安全感知、分析、响应、决策等能力。打造网络安全“靶场云”，建设数字孪生靶场，为城市安全能力验证等提供支撑。构建网络安全“服务云”，聚集智慧城市安全规划、建设、运营等服务资源，保障城市安全有序运行。

（三）产融合作深化行动

11.加大产业基金投入力度。引导国家制造业转型升级基金等政府引导基金向网络安全新技术、新模式以及融合创新领域

倾斜，适时推动设立国家级网络安全产业引导基金，加速新产品和服务在市场中成熟落地。鼓励地方政府将网络安全产业纳入政府引导基金投资范畴，支持本地区网络安全企业发展。

12.引导资本精准支持企业发展。鼓励各类资本建立科创基金，围绕产业科技创新和核心技术攻关，探索“科技捐赠”和知识产权、期权融资模式，引导资本市场投早投小，助力成长型企业强化技术优势，深耕细分市场，做专做精。鼓励基础较强的网络安全企业上市，支持领航企业通过战略投资方式整合资源，做大做强，提升网络安全生态引领能力。

13.强化产融合作机制建设。鼓励产融合作试点城市加大投入，深化网络安全产融合作。健全产融动态监测体系，定期开展网络安全领域风险投资、股权投资、企业并购、上市公司运营等动态监测，促进产融精准对接。推动建立符合网络安全产业特征、针对企业不同发展阶段的评价体系，支持开展高成长企业、高价值项目评估，协同做好信息共享和信用评价成果转换。

专栏 3　网络安全产业资本赋能工程
健全网络安全产融合作机制。充分发挥工业和信息化部国家产融合作平台作用，加强财税金融政策、融资需求、金融产品服务等信息交流共享，促进网络安全产融精准对接。 **积极开展安全产融服务。**成立“网络安全产业资本创新论坛”，积极开展上市辅导、企业路演、项目推介、融资培训等多层次产融对接活动和咨询服务，切实发挥充分应用金融资本对产业发展的助推升级作用。

探索开展网络安全保险。面向电信和互联网、工业互联网、车联网等领域，开展网络安全保险服务试点。加快网络安全保险政策引导和标准制定，通过网络安全保险服务监控风险敞口，鼓励企业构建并完善自身网络安全风险管理体系，强化网络安全风险应对能力。

探索开展网络安全企业价值评估。针对企业不同阶段及网络安全细分赛道，鼓励产业界和资本界联合建立价值评估模型和细化指标，探索开展高成长性企业清单、高价值项目目录发布工作。

（四）人才队伍建设行动

14.发挥领军人才带动作用。培育一批在理论研究、技术创新、成果转化、应用实战等方面能力突出的领军人才。鼓励企业、高校、科研机构等通过成立工作室、提供科研经费、股权激励、人才交流等多种方式，健全领军人才激励机制。鼓励高校、科研机构、企业等通过国际合作等多种途径，吸引全球高水平人才及创新团队。

15.深化产教融合协同育人。鼓励高等院校加强网络安全学科专业建设。推进网络安全校企合作，支持鼓励高等院校、研究机构与企业共建网络安全实训基地、联合实验室等，打造“双师型”师资队伍，增强网络安全人才实践能力。发挥行业特色高校、职业院校作用，发展更多网络安全技能型、服务型人才。积极开展网络安全教育培训活动，鼓励举办多层次、多元化网络安全能力竞赛，培育高素质网络安全人才。

16.推动开展网络安全人才能力评价。实施工业通信业职业技能提升行动，通过计算机技术与软件专业技术资格（水平）

考试、全国工业互联网安全技术技能大赛等方式，培养选拔网络安全专业人才。面向装备制造、原材料、消费品、电子信息等重点行业，构建“X+安全”人才评价体系，建立健全网络安全人才选拔评价机制。

（五）产业生态优化行动

17.引导网络安全产业集聚。打造“多点支撑、辐射全国、优势互补、协同发展”的网络安全产业园区布局，积极推进北京、湖南长沙国家网络安全产业园区建设，发挥成渝、长三角、珠三角等产业基础优势，加快国家网络安全产业园区布局。积极建设一批具有带动性、引领性的网络安全创新应用先进示范区。

18.推进创新联合体建设。鼓励基础电信运营商、行业用户、科研机构、高等院校、安全企业等建立网络安全联合创新中心、联合实验室等，强化基础网络安全理论研究，促进研究成果应用转化，提升网络安全领域关键核心技术创新能力。充分发挥网络安全相关行业企业联盟、协会作用，通过技术攻关、项目合作、人才培养、园区建设等多种形式，促进创新要素流动，整合技术优势和资源优势，激发创新活力。

19.培育公平竞争的市场环境。支持开展网络安全产品服务能力评价、网络安全工程建设与系统运行维护质量评价，和面向新技术新业务的安全评估。综合企业产品服务质量、漏洞贡献、威胁信息共享情况、恶意竞争等因素，加强企业信用体系

建设，逐步建立企业“红黑榜”，不断提升市场透明度，引导形成以产品服务能力为导向的良性市场竞争环境。

专栏 4　网络安全产业生态培育工程
建立网络安全产品和服务能力评价制度。聚焦网络安全产业链上下游关键环节技术产品，绘制网络安全产业链图谱，持续开展网络安全产业重大风险研判。综合网络安全产品关键功能性能、能力成熟度、应用效果，以及网络安全服务水平等因素，分别制定网络安全产品和服务能力评价规范，公开发布评价结果。 **完善网络安全威胁信息共享服务体系和机制**。建立驱动漏洞、恶意程序、恶意地址、攻击行为等威胁信息挖掘、披露、流转和利用的规则机制，鼓励网络安全企业、行业用户、科研机构、高校积极参与信息共享，提升威胁信息要素聚集水平与服务能力。 **强化先进技术应用示范推广**。面向 5G、车联网、工业互联网、物联网等重点方向，开展优秀安全产品及解决方案遴选，通过交流论坛、举办比赛、供需对接等方式，促进试点示范项目在各重点行业领域应用推广，持续激发创新活力，促进成果转化。 **培育网络安全优质企业标杆**。鼓励企业加大研发投入，强化知识产权保护和技术创新。鼓励综合实力强，在国内外技术、标准、市场等方面具有较强影响力的企业进一步整合产业链、供应链和创新链，成为产业链领航企业。针对网络安全产品细分市场优秀企业，通过政策指导、项目倾斜、人才培育等方式，强化对技术研发、产品推广、供需对接等的支持，加快培育网络安全单项冠军企业和专精特新“小巨人”企业。

三、保障措施

（一）加强组织领导。各地工业和信息化主管部门、通信管理局要加强组织领导，强化部门协同，积极推动将网络安全产业纳入地方“十四五”总体规划及有关专项规划重要内容。

加强对不同行业、不同领域、不同主体网络安全建设的分类指导，推动网络安全产业发展差异化布局，建立健全网络安全保障体系，营造有利于网络安全产业发展的良好环境。

（二）强化政策引导。充分利用网络安全技术应用试点示范、首台（套）、专项项目等现有政策，推动地方结合本地实际情况，针对不同发展阶段的网络安全企业，在财政金融、人才培育、产业集聚等方面研究制定有针对性的支持政策，强化政企协同和部省联动，形成工作合力，推动网络安全产业与地方数字经济发展紧密融合。鼓励地方在财政投资的信息化项目中同步配套建设网络安全技术措施，在项目验收阶段加强对网络安全方面的评审。鼓励重点行业企业加大网络安全投入，单独列支网络安全预算，推动网络安全技术、产品和服务部署应用。

（三）增强产业协同。成立工业和信息化部网络安全产业高质量发展专家咨询委员会，对重大问题和政策实施情况提出咨询建议。充分发挥产学研用资各方力量，强化供需对接，协同推进标准制定、人才培养和成果转化，加强行业自律，营造健康有序、良性发展的产业生态。

（四）推进国际合作。充分利用双多边机制，积极参与网络安全国际规则和重点领域安全国际标准制定，加强网络安全政策、法规、产业交流合作。支持企业设立海外研发中心、联合实验室，支持各类网络安全会议论坛、展示展览等交流活动，着力构建多层次、常态化产业合作交流机制。