成都市网络信息安全产业发展规划

（2018–2022 年）

2018 年 9 月

目　录

网络安全已经成为国家安全的重要内容，没有网络安全就没有国家安全。网络信息安全产业为国家关键信息基础设施提供安全产品及服务，是保障国家网络安全的重要支撑。为科学规划与引导成都网络信息安全产业健康、持续发展，根据党的十九大会议、省第十一次党代会、市第十三次党代会精神，以及《中华人民共和国网络安全法》、《四川省信息安全产业发展规划(2015-2020 年)》和《成都制造 2025 规划》的要求，特编制本规划，规划期为 2018 至 2022 年。

一、基础现状

（一）现实基础

近年来，成都不断加快网络信息安全产业基地建设，重点突破了一批关键共性技术，积极引进龙头企业和重点项目，大力培养网络信息安全高端人才，推动网络信息安全产业持续、快速发展，助力网络信息安全企业做大、做强、做优，不断夯实网络信息安全产业基础。

1．政策环境显著优化

为促进网络信息安全产业快速发展，国家先后出台了《中华人民共和国网络安全法》、《国家网络空间安全战略》等一系列法律和顶层设计文件。工业和信息化部也印发了《信息通信网络与信息安全规划(2016-2020 年)》、《工业控制系统信息安全行动计划（2018-2020 年）》、《工业互联网发展

行动计划（2018-2020 年）》等一系列网络信息安全领域规划文件，紧扣网络信息安全工作面临的重大问题，对网络信息安全工作进行统一谋划、设计和部署。

响应国家对网络信息安全产业的战略部署，四川省成立了由省领导牵头，有关部门、地方和产学研单位组成的信息安全产业发展推进小组，将网络信息安全产业纳入重点发展的五大高端成长型产业之一，并制定了《四川省信息安全产业发展规划（2015-2020 年）》和《四川省信息安全产业发展工作推进方案》，提出将四川省建成国家网络信息安全产业高地，设立了集成电路和信息安全产业投资基金，为网络信息安全产业发展提供资金保障。

为充分发挥成都市网络信息安全优势，促进网络信息安全产业快速发展，成都市出台了多项网络信息安全产业扶持政策，包括《成都市促进五大高端成长型产业发展的若干专项政策》（成办函〔2016〕5 号）、《关于创新要素供给培育产业生态提升国家中心城市产业能级若干政策措施的意见》（成委发〔2017〕23 号）和《关于深入实施“创业天府”行动计划加快打造西部人才核心聚集区的若干政策》（成委发〔2016〕1 号）等，从技术创新、人才培养、产业协同、资金支持等多个方面，推动构建特色鲜明、优势突出的网络信息安全技术、产品和服务体系，巩固和提升成都在全国网络

信息安全产业版图中的地位。

2．产业自主创新能力较强

成都是科技部授牌的国家信息安全成果产业化基地，建成了西部首个信息安全产业园区，拥有超过 40 个重点（工程）实验室、工程（技术）研究中心、企业技术中心等国家和省级信息安全创新载体，聚集了中国网安，中国电科集团 10 所、29 所、战略支援部队第五十七研究所、中科院成都计算机应用研究所等众多网络安全科研院所，以及亚信网络安全产业技术研究院等企业研究机构，形成了较为完善的网络信息安全技术研发体系。

网络信息安全人才培育体系健全，拥有数量众多的网络信息安全人才。四川大学、电子科技大学、西南交通大学、成都信息工程大学等拥有网络信息安全学科的科研院校已经形成了完整的涵盖博士、硕士、学士等各层次学历培养的网络信息安全专业人才输送体系。国家保密局、四川省国家保密局和四川大学三方共建了四川大学国家保密学院，以培养信息安全（保密技术方向）专业人才。成都工业职业技术学院、四川邮电职业技术学院等高职院校也开设了网络信息安全专业班，国信安基地、启明星辰安全培训中心、亚信网络安全产业技术研究院、蓝盾学院等企业培训基地也在开展网络信息安全技术应用型人才培训。截至 2017 年底，全市

网络信息安全从业人员超过4万人，各类网络信息安全认证人员逾 8000 人，为网络信息安全产业发展积累了雄厚的人才实力。

3．产业集聚发展效应明显

2017 年，成都网络信息安全产业规模达到 187.88 亿元，同比增长 33.35%；实现利润 32.6 亿元，同比增长 64.98%，在全国各城市中位居前列。

成都拥有上百家网络信息安全企业，其中，全国网络信息安全前 50 强企业数量达到 24 家，增长率前 10 强企业 5 家。高新区建有“国家西部信息安全产业园”，聚集了亚信安全、卫士通、长城网际、四川无声、中科慧创等知名企业。双流区拥有国家级网络信息安全龙头企业中国网安，聚焦工控安全、云计算与大数据安全等领域，志在打造国家级军民融合信息安全产业园区。天府新区在成都科学城聚集了启明星辰等知名企业。武侯区重点打造无线电监测相关产业，聚集了华日、佳发安泰、大公博创、中星世通等国内领军企业。

成都建有多个网络信息安全运营中心和平台。2014 年 10 月，长城网际在蓉建成国家级信息安全服务平台西南中心，也为成都信息安全监测及应急响应管理平台提供服务；2016 年，亚信安全在蓉投资建成信息安全公共服务平台、网络安全态势感知运营中心和高级威胁调查取证运营中心；

2017 年 12 月，启明星辰在成都建成了国内规模最大的安全运营中心，助力成都成为国内重要的信息安全运营服务基地。

4．部分领域处于全国领先地位

在自主可控方面，成都聚集了三零嘉微、紫光展锐、九洲迪飞等自主研发能力较强的厂商。其中，三零嘉微在信息安全与通信保密芯片领域的技术和产品处于国内领先地位，在专用芯片设计领域已经拥有多项技术发明专利；九洲迪飞在微波射频方面技术达到了国内先进水平，产品广泛用于雷达、航空、航天、船舶、陆航、通信、电子对抗等领域。

在传统安全方面，卫士通的加密产品已经达到世界先进水平；华日、大公博创等企业在电磁防护方面具有较强影响力；启明星辰、亚信安全、卫士通、四川无声等企业在终端安全产品方面具有一定优势；卫士通、启明星辰、亚信安全、迈普通信、天融信等在网络安全产品方面具有较强实力；中国网安、亚信安全、久远银海、融微软件、启明星辰、知道创宇等企业在网络监测预警方面具有较大国内影响力；中国网安、卫士通、启明星辰、亚信安全、思维世纪、四川无声等企业构建了面向多个行业的安全整体解决方案，在党政、金融、电力、能源、交通等行业得到应用。思维世纪、四川无声、无糖信息、肆零肆科技、永信至诚等企业在渗透测试

领域具有较强实力；卫士通、启明星辰、亚信安全、长城网际等企业在安全集成方面实力较强。

在新兴领域安全方面，启明星辰、亚信安全、长城网际等企业在云计算安全方面具有较强实力；上海云盾、知道创宇等企业在移动互联网安全方面具有坚实基础；启明星辰、四川无声、亚信安全等企业在大数据安全方面具有很大优势；成都反应链、成都布洛克在区块链领域具有一定影响力。

（二）主要问题

近年来，成都网络信息安全产业虽然有了长足的发展，但产业发展的深层次问题和结构性矛盾仍然存在，主要表现为：网络信息安全产业支持政策亟待完善，网络信息安全产业链有待进一步完整，综合性的大型本地企业数量不多，自主创新能力优势不明显，云计算、大数据、工控系统等领域安全意识薄弱、重视程度有待提升，网络信息安全人才流失严重等等。这些问题严重制约了成都网络信息安全产业由大变强，需要在未来五年着力解决。

二、指导思想和发展原则、目标

（一）指导思想

深入贯彻落实党的十九大精神和习近平总书记关于“自主创新推进网络强国建设”的要求，根据四川省第十一次党代会、成都市第十三次党代会精神，围绕国家对网络信息安全

保障的新要求，以推进成都网络信息安全产业快速发展为目标，加强关键核心技术突破，创新服务模式，培育骨干企业，完善产业发展环境，培育产业新业态，释放产业活力，为成都网络信息安全产业持续健康发展注入新动力。

（二）发展原则

安全可控。鼓励和支持核心芯片、基础软件、整机等核心技术自主创新，研发具有自主知识产权的基础软硬件产品。着力推进自主核心技术产品的产业化和应用推广，建立完整的网络信息安全技术、产品、服务和标准体系，保障新技术、新应用的安全可控，保障基础信息网络和重要信息系统的安全可控，为国家、企业和个人的网络信息安全保障提供产业支撑。

创新驱动。加快政策与机制创新，大力推进大众创业、万众创新，全面提升技术、人才、资金的供给水平，营造创新要素互动融合的生态环境。促进政产学研用联动，提高自主创新能力，以技术创新带动产品创新、模式创新，构建以企业为主体的网络信息安全产业创新体系。聚集各方资源，加大网络信息安全技术创新投入力度，突破影响产业发展的核心技术和关键产品，创新服务模式，占领价值链高端，提升产业核心竞争力。

应用牵引。面向国家安全战略、国家信息化建设和两化

深度融合带来的网络信息安全保障需求，鼓励和支持采用安全可控的产品和服务，加快安全可控网络信息安全技术、产品和服务的应用推广。强化需求侧政策引导，关注工控系统、云计算、大数据、物联网、移动互联网等新兴领域安全需求，推进新产品、新服务的应用示范，加快培育和完善网络信息安全产业链，不断优化网络信息安全产业结构，促进全市网络信息安全产业持续、健康发展。

集聚发展。营造良好的产业发展环境，加强网络信息安全产业平台建设，吸引国内外网络信息安全企业总部、科研中心落户，鼓励企业整合并购，培育行业龙头企业和“隐形冠军”，带动成都网络信息安全产业的集聚发展。以产业链和创新链协同发展为途径，加强关联产业协同发展，打造网络信息安全产业集群，构建产业生态圈，形成创新经济集聚发展新格局。

（三）发展目标

到 2022 年，将成都打造成为西部领先、国内一流的网络信息安全产业高地，为建设“中国网络信息安全之城”提供产业支撑。

——产业规模。打造网络信息安全产业集群，全市网络信息安全产业规模超过 500 亿元。

——技术创新。重点实验室、企业技术中心等国家和省

级网络信息安全创新载体达到 50 个；网络信息安全企业研发投入占比达到 4%；建成国内网络信息安全人才高地，累计引进培养达到 3 万人。

——**行业实力。**引进 10 家以上国内领军企业，培育 3 至 5 家国内领军企业和独角兽企业，产业规模超过 500 亿元。在通用芯片、密码、电磁防护、大数据安全、工控安全、云计算安全、安全服务等领域达到国内领先水平，形成具有国际竞争力的现代产业体系。

——**服务能力。**聚集 5 至 10 个面向全国提供网络信息安全服务的运营中心，新增 5 至 10 个国家级共性基础服务机构，建成全市统一的网络信任服务体系。

三、主要任务

（一）加强核心技术创新

加强关键核心技术研发。依托成都企业在密码方面的优势，加快基于商用密码产品的研制，逐步实现国产高性能密码产品替代；鼓励电磁防护优势企业，加快电磁防御、系统级电磁兼容测试与整改解决方案、电磁防御系统等产品的研发；完善自主可控产业链，加速突破芯片、操作系统、中间件以及服务器等整机设备的研制；加强对数据脱密、脱敏，存储备份一体化设备的研发和制造；大力发展工控安全领域高可用、高稳定、高性能防火墙、入侵防御、安全隔离与信

息交换系统；加快虚拟化安全、数据安全隔离与加密、安全中间件、数据备份与恢复等云计算安全关键技术研发。积极布局量子通信、区块链、人工智能等前沿技术领域，提升关联分析、机器学习、智能感知等技术能力。

加强创新载体建设。充分发挥密码、电磁防护、数据安全、态势感知等安全行业骨干企业的创新主导作用，形成一批有国际竞争力的创新型领军企业。引导企业与知名高校、研究院所深度合作，共建工业信息安全制造业创新中心等产学研用协同创新机构和产业创新联盟。围绕产业创新链联合开展课题攻关、技术创新和成果转化，形成一批创新资源集聚、组织运行开放、治理结构多元的网络信息安全创新平台。利用军工科研院所分类改革、军工企业市场化改革等多项全国试点示范落地四川的政策优势，推进中国电子和中国电科等央企军工集团与成都深度合作，共同推动网络信息安全领域重大科研项目、军民融合研究院和产业基地建设。

推进科技成果产业化。建立完善科技成果信息发布和共享平台，健全以技术交易市场为核心的技术转移和产业化服务体系。完善科技成果转化协同推进机制，引导产学研用按照市场规律和创新规律加强合作，鼓励安全企业和社会资本建立一批从事技术集成和工程化的实践基地。搭建网络信息安全领域科技成果军民双向转化渠道，推进军民科技协同创

新和科技创新资源共建共享，建设具有成都特色的网络信息安全军民融合创新体系。

（二）巩固产业发展优势

促进产业集聚发展。支持高新区南部园区、天府新区成都直管区、双流区依托现有产业基础，加快发展步伐，打造网络信息安全产业主体功能区，并逐步发展成为网络信息安全的主体聚集区与核心发展区，支持武侯区建设以传统安全产品为主的产业园区，支持锦江区建设金融安全产业园，助推成都网络信息安全产业聚集发展。

培育行业龙头企业。构建多领域、分阶段、递进式的网络信息安全企业培育体系，支持企业做大、做强。在应用安全、边界安全、数据安全等领域中，重点挖掘、甄别一批“隐形冠军”，培育其快速成长为独角兽企业和领军企业。鼓励和引导企业兼并重组，支持龙头骨干企业开展并购，以资本为纽带推进资源整合及产业融合，加快发展和形成一批掌握关键核心技术、创新能力突出、品牌知名度高、国际竞争力强的安全大公司。

扶持中小安全企业。鼓励企业之间错位发展，支持龙头企业牵头建立创新创业孵化基地，带动相关中小企业发展，提高全市网络信息安全产业整体竞争力。在云计算安全、工控安全、大数据安全、态势感知等领域，加强企业间的联合

和协作，引导中小企业向“专、精、特、新”方向发展，重点培育一大批专注核心主营业务、成长质量高、创新能力强、经济效益好、拥有自主品牌、具有示范带动作用的中小安全企业群体，使其发展成为各细分行业的领袖和冠军，与大企业共同构建合理分工、优势互补的产业生态链体系。

（三）大力发展安全服务

打造国内安全运营服务高地。鼓励国内网络信息安全领军企业在成都建设面向全国的信息安全服务运营中心，重点发展安全咨询、安全测评、安全监测、安全运维、安全培训等安全服务方向。引导党政部门和企事业单位从采购单一安全产品向采购安全产品和安全运营服务相结合的模式转变，促进网络信息安全运营与智慧城市建设深度融合。加快成都网络信息安全运营服务产业的规模扩大、应用升级和技术创新，不断提升成都在国内网络信息安全运营的服务能级。

建立国内一流的安全服务体系。完善覆盖全产业链的能力评估、安全测评、仿真测试、审查认证、元器件检测及筛选、产品可靠性与环境试验等共性基础服务能力，形成立足成都、面向全国的国内一流服务体系。争取国家支持在蓉开展商用密码产品检验检测专业化服务试点，组建商用密码产品第三方检测中心，积极引进国家工业控制系统与产品安全质量监督检验中心、国家电子元器件失效物理重点实验室等

一批专业测评机构。

强化网络信任服务体系建设。依托现有电子认证体系，针对各类数据平台和网络应用，支持电子认证服务机构提供异构、跨域、可信的身份认证、权限管理、访问控制、安全审计、责任认定等网络信任服务，引导规范数字证书的使用与管理，推进数字证书应用，建设全市统一的网络信任服务体系。

（四）深入开展试点示范

自主创新和军民融合创新示范。加强自主芯片、基础软件、安全可靠终端、智能应用系统等产品研发，出台政府采购政策，推进自主产品在党政机关、军队和关键信息基础设施行业的应用示范。通过建设军民融合研究院、产业基地和科技成果双向转化平台等，加快“军转民”和“民参军”步伐，加快军民融合创新，推进军民融合技术产品应用。

重点领域安全应用示范。在量子保密通信、区块链安全、工业信息安全、云计算与大数据安全等重大应用领域，实施网络信息安全应用试点示范工程，形成具有示范和推广价值的典型经验。选择电子政务及交通、教育、医疗等重要政务和民生领域，开展大数据安全应用示范，推广数据安全技术和解决方案，加强政务数据和公共数据的安全防护。

新兴领域安全应用示范。支持国内领先的人工智能、区

块链、机器人等企业，与在成都落户的网络信息安全企业进行合作，开展新兴领域安全前瞻性研究，研发新兴领域安全技术产品和解决方案，推广网络信息安全技术产品和解决方案应用。支持建设新兴领域安全检测认证等公共服务机构。

（五）加快建设人才队伍

着力引进高端人才。设立网络信息安全人才引进专项资金，依托国家“千人计划”、四川省“千人计划”和“蓉漂计划”等人才引进工程，围绕成都网络信息安全人才需求，加快实施国内外高层次创新创业领军人才和高端人才的引进计划。充分发挥校友会、行业协会等团体的桥梁纽带作用，重点引进网络信息安全领域的职业经理人、团队组织者等高端运营人才，以及支撑企业创新发展的高端技术人才。完善人才激励和保障机制，支持专业人才以知识、技术等参与收益分配，探索期权、期股、延期支付等长期激励手段，确保人才可以留得住、用得好。

加强院校培养力度。依托四川大学、电子科技大学、西南交通大学、成都信息工程大学等省内高校，加大网络信息安全学科建设力度，争创一流学科专业，积极探索人才定制化培养、定期培训进修等多种教育创新合作模式机制，着力提升成都网络信息安全人才培养的数量和质量。鼓励高校创新人才培养模式，建立健全多层次、多类型的网络信息安全

人才培养体系。

发展职业教育培训。依托成都工业职业技术学院、四川邮电职业技术学院等职业学院，重点培训专业技术人才、行业应用人才。支持专业机构开设网络信息安全人才培训项目，开展基础安全培训、持证培训、实战性培训。鼓励高校与企业联合建立实习培训基地，强化网络信息安全人才工程实践培养。支持具备国家相关部门认证授权的安全企业开展网络信息安全人才培训业务。

四、发展重点

基于成都网络信息安全产业发展现状和技术发展趋势，结合现有产业基础和需求，提出未来五年成都网络信息安全产业发展重点，主要包括自主可控、物理安全、密码产品、身份与访问控制、安全测评、安全监测、工控安全、云计算安全和大数据安全等。

（一）自主可控

依托优势企业建设集成电路设计、研发和生产基地，大力提升集成电路设计水平，突破核心通用芯片、以及智能电视核心和外围芯片、北斗导航基带和射频芯片等专用芯片研制，提升封装产业和测试的自主发展能力；加大对操作系统、数据库、中间件、办公软件等基础软件的研发，重点突破工业控制类嵌入式实时操作系统、云安全操作系统、云计算中

间件、智能手机操作系统等国产基础软件；推进具有自主知识产权的通用服务器、存储设备、终端产品等整体设备的研制，大力发展北斗、高分手持和车载终端产品以及安全家庭信息终端产品，鼓励企业加快工业控制计算机等行业专用计算机产品，大型服务器、海量存储等云计算基础设备，高端容错计算机、融合架构服务器、大数据存储设备和高密度、低成本的通用型服务器、大容量存储服务器等大数据基础设备的研制。

（二）物理安全

鼓励电磁防护优势企业，围绕党政、军队、重点行业的重要场所电磁防护、重要系统电磁兼容防护以及电磁空间频谱安全监测、管控等方面的要求，加快电磁防御、系统级电磁兼容测试与整改解决方案、电磁防御系统建设等产品的研发与应用，为党政、军队及行业用户提供“励电磁防+电磁安全”的多层次全方位电磁防御系统级解决方案。

（三）密码产品

鼓励企业加大对密码技术的研发，在密码算法理论、标准、应用模式上开展深入研究，重点突破量子加密、轻量级密码算法、高效全同态密码技术、生物密钥技术、基于属性密码技术等一批新型密码技术；推动基于国产商用密码的产品研制，包括密码系统及密码器、密码算法硬件实现、电子

证书认证系统、安全网关等技术和产品等，逐步实现国产高性能密码产品替代；推进密码技术与大数据、云计算等新兴技术的结合，带动密码技术产品在新兴领域的应用。

（四）身份与访问控制

引进一批 FIDO、生物特征识别、用户行为分析等身份认证技术研究和制造企业，鼓励企业加大对多维度、综合性的可信身份认证技术的研发；依托本地优势企业加大对指纹识别芯片、金融 IC 卡、加密机、SSL/VPN 服务器、签名验签服务器等可信身份软硬件产品的研发和生产；鼓励电子认证技术相关企业积极开展基于云计算等新模式下的身份认证、访问控制、授权管理等技术的研发。

（五）安全测评

重点开展网络信息安全产品测评、等级保护、风险评估等服务，建设安全事件库、安全漏洞库、恶意代码库、软件补丁库等数据库。依托优势企业开展对防火墙、入侵监测、安全审计、网络隔离、VPN、安全管理等信息技术产品的安全性检测。引进和培育一批企业开展信息系统的安全性测试、评估，包括信息系统安全等级保护测评、信息安全风险评估、信息系统安全保障能力评估、信息系统安全方案评审等服务。

（六）安全监测

依托现有监测平台，建设全方位网络信息监测预警保障体系，为政府部门、企事业单位及社会公众提供网络信息安全监测服务，提高金融、移动互联网、电子政务、电信运营商、医疗、交通等各行业的风险监测水平，提高网络信息安全保障能力；依托现有态势感知中心，建立面向重要信息系统和关键信息基础设施的态势感知网络，并对外提供信息化基础设施安全保障建设服务、集成服务，舆情引导分析与大数据安全态势分析综合服务；鼓励企业建立网络信息安全态势感知系统，加强机器学习、数据建模、行为识别、关联分析等技术的研发，加强病毒库、木马库、特征库、规则库、恶意 URL 库的建设，提高对木马、蠕虫、暗链、舆情、漏洞发现与验证水平，提高威胁处理的应急能力，缩短响应时间。

（七）工控安全

引进一批从事工业防火墙、网闸、安全审计、漏洞扫描、异常流量清洗、安全监测、网络交换机、可信传感器、控制器、行为监管及 APT 防护等主流设备和系统的研发和生产企业；大力发展高可用、高稳定、高性能防火墙、入侵防御、安全隔离与信息交换系统等工控产品；完善工控系统安全测评体系，开发针对工控安全的漏洞扫描及配置核查、工控现场安全基线及漏洞检测等工具，开展工控安全防护能力评

估，提升各行业工控系统信息安全水平。

（八）云计算安全

鼓励企业对虚拟机安全防护与检测、虚拟机安全监控和虚拟机隔离机制等关键技术的研发，重点发展可信平台模块的虚拟服务器，研发跨平台的虚拟化技术；加快虚拟化安全、数据安全隔离与加密、安全中间件、数据备份与恢复等云计算安全关键技术研发及产业化；鼓励企业开展云灾备服务，采用先进、安全、可靠的数据备份和数据复制技术，建设可管理、可运营的灾备服务，依托云计算环境为用户提供数据灾备服务，或为迁移到云上的应用系统提供不同等级的同城或异地数据灾备服务。

（九）大数据安全

鼓励优势企业加强对共性基础技术研发，重点突破数据存储安全、数据清洗等核心技术研发和创新；加快数据流动监控与追溯、数据安全隔离与加密、数据隐私保护、数据备份与恢复、安全智能感知等大数据安全技术研发及产业化；支持企业研发面向云平台安全防护、大数据安全管理的网络安全产品；推动基于大数据的安全测评服务；建设大数据安全开发与治理中心、大数据安全实验室等，推动安全态势大数据分析。

五、重大工程

（一）自主可控产业培育工程

积极引进和培育集成电路设计、制造和封测企业，提升安全可控 CPU、DRAM 芯片等关键产品设计开发能力，支持先进制造工艺、存储器、特色工艺等生产线建设，提高代工企业及第三方 IP 核企业的服务水平，推动封装测试、关键装备和材料等产业快速发展，推动重点环节提高产业集中度，打造中西部集成电路中心。

以成都为主打造基础软件开源社区，针对服务器操作系统、移动操作系统、云操作系统、实时操作系统、大型关系型数据库、高性能分布式数据库等关键基础软件，抓住技术变革的关键节点，依托自身应用需求体量优势，充分利用全球资源，整合国内外顶尖技术专家能力，缩短产品迭代更新周期，打造国际一流的基础软件产品。

整合产业链，推动自主可控信息技术产品集成适配，优化提升自主可控芯片、操作系统等关键部件产品，提高整机产品的可用性，快速增强产业能力。鼓励和支持企业开展集成创新，充分利用现有自主可控信息技术产品，针对云计算、大数据等新兴应用需求，研制专用服务器、存储设备等，通过集成创新弥补单点缺陷，并加快应用推广。

（二）军民融合创新工程

结合军工科研院所分类改革和军工企业混合所有制等

多项全国试点示范工程，依托中国电子、中国电科等央企军工集团，建设军民融合研究院和产业基地，加大网络信息安全军民两用技术产品的研发生产，推动网络信息安全领域重大科研项目落地成都，打造国家网络信息安全军民融合创新发展聚焦区。

争取更加开放的政策支持，建设网络信息安全领域科技成果军民双向转化服务平台，推进军民科技协同创新和科技创新资源共建共享，建设具有成都特色的网络信息安全军民融合创新体系，培育军民两用人才队伍，形成军民技术、人才、产业深度融合发展新格局。

（三）检测认证等第三方服务培育工程

依托网络信息安全科研院所、行业龙头企业等资源，通过政府引导、社会投资方式，建设网络信息安全公共服务集聚区，重点培育检测认证、仿真测试、技术展示、教育培训、创业孵化等公共服务，立足成都、面向全国提供服务，形成国内一流的服务能力。

聚焦智能网联汽车、工业控制系统、机器人等新兴领域，引入中国软件评测中心等外部资源，建设 4-5 家网络信息安全检测认证服务机构，提供网络信息安全产品检测、系统测评、等保咨询、风险评估等服务。

按照“前瞻设计、国内一流”原则，建设公共、专业与特

种靶场相结合的网络攻防对抗靶场，提供安全攻防演练、产品研发试验、技术演示验证和人才教育培训等服务，推动成都网络信息安全技术创新、科学研究、人才培养进入国内一流行列。

（四）网络可信服务建设工程

依托电子认证服务机构、大型互联网公司等网络身份服务提供商，建设网络可信身份服务集聚区，推动网络可信身份在安全性要求较高的政务、金融、商贸等领域应用，为政务、金融等活动的安全开展提供保障。

整合现有公安、工商、电信运营商等多种网络可信身份数据资源，建成可信身份基础数据管理平台，向政府部门提供基础数据共享开放服务，具备对社会各类身份服务商可信身份数据资源的对接和管理能力。

支持有能力的网络身份服务提供商建设具有多属性认证、跨平台认证、多级别安全认证、应用接入方便等优势的网络可信身份服务平台，完成对网上行为主体的多途径、多角度、多级别的身份属性信息的收集、确认、评价及应用，实现身份认证凭证之间的互通互认，形成立足成都、覆盖全国的网络可信身份服务能力。

（五）工控安全技术应用示范工程

由市经信委牵头、联合各行业主管部门，在装备制造、

电子信息、生物医药、能源化工等重点行业，开展工控安全技术应用示范。

根据示范场景的需求，组织开展工控防火墙、网闸、漏洞扫描以及工业云、工业大数据安全防护等工控安全技术产品研发，根据重点行业应用效果，不断改进和提高相关组件、工具、控制装备的行业适配性，形成重点行业工控安全防护整体解决方案。

总结试点经验，研究提出工控安全技术产品相关标准规范，将试点成果向四川省其他地区、乃至全国范围内推广，形成示范效应。

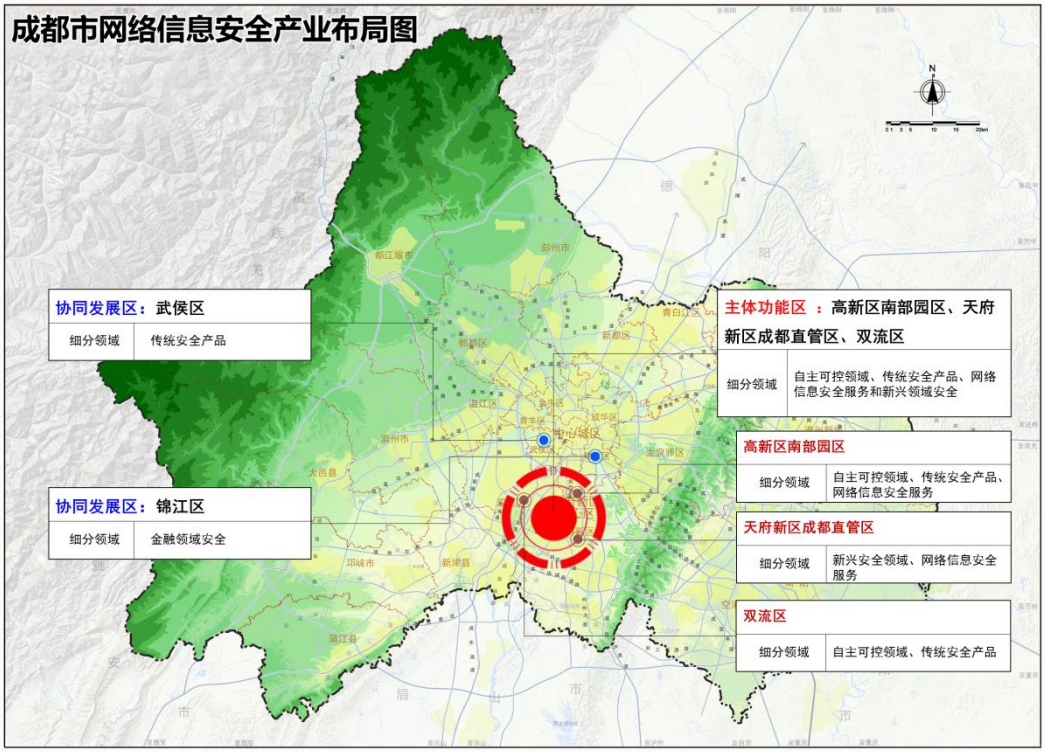
（六）政务数据安全应用示范工程

依托成都市公共数据开放平台，建设政务数据云共享平台，加快重要政务应用和数据的云端迁移，并通过统一政务数据标准、建立政务数据共享制度等措施，将各部门的政务数据进行共享和交换，强化政务数据共享交换过程中的个人信息保护力度，实现政务数据的安全汇聚和共享。

重点加强动态文档透明加密技术、虚拟化技术、云端数据安全技术、智能加密技术等技术研发，加强政务数据安全防护技术手段建设，定期开展针对政务数据的安全审计，及时发现并修补政务数据安全防护中的问题，采取改进措施，提升对重要政务应用和数据的安全防护能力。

六、空间布局

依托成都产业现有基础，统筹区域优势产业，合理优化空间布局。重点在高新区南部园区、天府新区成都直管区、双流区打造网络信息安全产业的主体聚集区与核心发展区，武侯区、锦江区依托各自现有产业基础和优势，发展具有区域特色的网络信息安全产业。到 2022 年，全市网络信息安全产业形成“1+2”的空间布局。



“1”是指一个核心发展区，主要包括高新区南部园区、天府新区成都直管区、双流区。重点支持自主可控领域、传统安全产品、网络信息安全服务和新兴领域安全四个网络信息安全领域，形成网络信息安全产业的主体聚集区与核心发展区。

高新区南部园区：依托现有产业基础，建设以网络信息安全技术创新为核心，自主可控领域、传统安全产品和网络信息安全服务为主体的产业园，重点发展密码产品、身份与访问控制、安全测评、工控安全、云计算安全、大数据安全等领域。

天府新区成都直管区：以成都科学城为主要载体，建设以创新研发、新兴领域安全、网络信息安全服务为主体的产业园，重点发展移动互联网安全、大数据安全、云计算安全等新兴领域安全，同步开展安全咨询、安全集成、安全监测、安全测评等网络信息安全服务。

双流区：以中国电科（成都）网络信息安全产业园、成都芯谷为主要载体，建设以自主可控领域、传统安全产品为主体的产业协作区，重点发展自主可控芯片、数据库、服务器、终端、整机等安全可控产品，同步推进工控安全、云计算安全、大数据安全等新兴领域安全。

“2”是指两个产业协作区，包括武侯区和锦江区。

武侯区：建设以传统安全产品为主的产业园，重点发展无线电监测、抗电磁干扰等传统网络信息安全产业。

锦江区：建设金融安全产业园，重点发展征信大数据、风险控制等金融安全服务。

七、保障措施

（一）强化组织领导

成都市网络信息安全产业推进工作领导小组统筹领导并协调推进全市网络信息安全产业发展工作。各区（市）县根据本规划，结合本地产业发展重点，制定具体实施方案，细化目标和举措，定期总结上报情况，确保各项任务落实到位。建立网络信息安全产业专家库，发挥专家在重大政策制定、重大项目评审等方面作用。

（二）加强政策扶持

发挥政府资金引导作用，统筹现有专项资金，创新支持方式，重点支持技术研发、项目孵化、产业协同、应用示范、公共服务、企业发展等。适时制定云计算、人工智能、区块链等新兴领域安全产业发展专项政策，在企业设立、投融资、税收、人才引进等方面给予优惠。扩大政府购买网络信息安全服务范围，鼓励和引导重点行业企事业单位采购具有自主知识产权的网络信息安全产品及服务。

（三）优化营商环境

围绕《中华人民共和国网络安全法》和相关法律法规的落实，适时出台网络信息安全相关管理办法和规定，严格行政执法。坚持放管结合，健全网络信息安全市场准入和退出机制，鼓励各类市场主体公平竞争、优胜劣汰，维护公平、诚信、有序的市场环境。规范发展中介服务，支持设立网络

信息安全企业社区等社会团体，汇聚投融资机构、战略咨询机构、创新创业平台、龙头企业等主体，建立常态化沟通交流机制，为企业发展提供高端化、专业化、集成化服务。

（四）做好实施评估

建立网络信息安全产业统计监测和指标评价制度，科学评价产业运行情况。在政府部门定期开展规划实施监督考核，考核结果纳入各相关单位的目标考核体系，对认真落实意见的单位和人员予以通报表彰。建立重大工程项目动态评估机制，按年度开展重大工程项目实施进度评估，对不能按既定目标完成任务的承担单位，追究相应责任并纳入退出机制。

附件

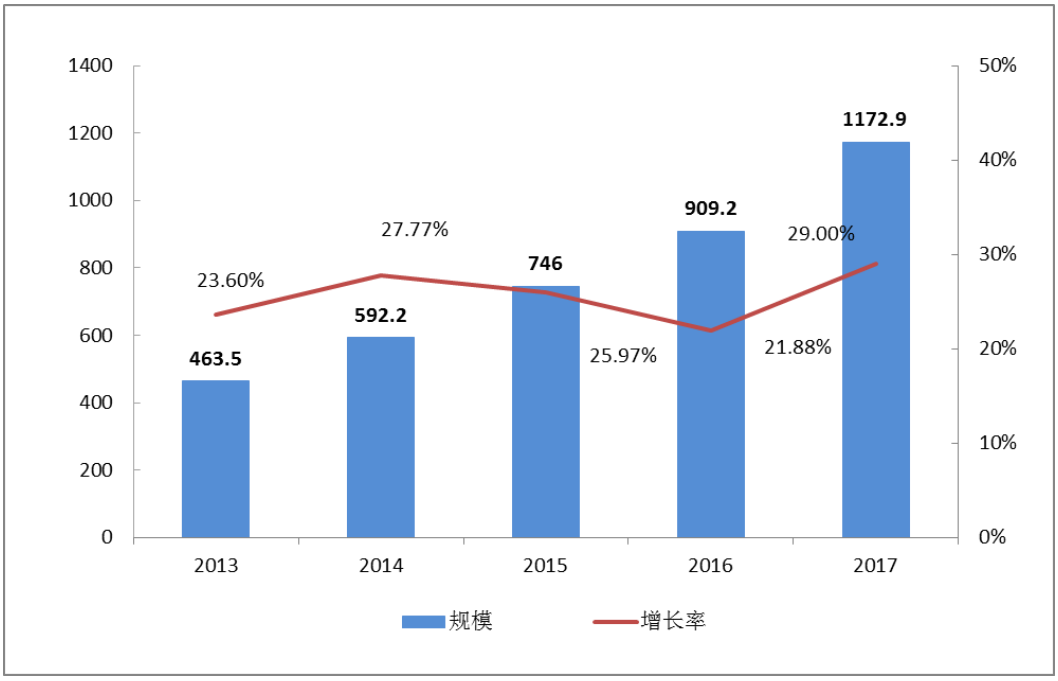
我国网络信息安全产业发展现状及趋势

一、产业现状

产业规模。在国家政策的驱动下，网络信息安全产业投资力度不断加大，产业规模实现快速增长。根据赛迪智库统计，2017 年，我国网络信息安全产业规模达到 1172.9 亿元，同比增长 29%，如下表和下图所示。

2013-2017 年我国网络信息安全产业规模和增长率

年份	2013	2014	2015	2016	2017
产业规模（亿元）	463.5	592.2	746	909.2	1172.9
增长率(%)	23.6	27.77	25.97	21.88	29



2013-2017 年我国网络信息安全产业规模及增长率

区域分布。北京在我国网络信息安全产业中处于龙头地位，成都、上海、广州等城市紧随其后，天津、杭州、武汉、重庆等其他城市借助国家政策支持和网络信息安全需求，也在积极布局发展。

二、发展趋势

自主可控是网络信息安全产业发展的必然趋势。为保障网络信息安全，一方面要大力发展具有自主知识产权的网络信息安全技术产品，实现我国重要网络信息安全系统技术和装备的国产化；另一方面要大力支持自主可控网络信息安全产品的推广和使用，不仅在事关国家网络信息安全的要害部门，更在百姓日常生活中大力推广和应用。

涉密网络信息安全已成为国家安全战略的重中之重。在信息时代，以声、光、电、磁等多种形式存储的涉密信息成为国家秘密的主要存储载体，国家秘密事关国家安全和利益，是国家的重要战略资源，国家秘密一旦泄漏，必将直接危害国家的政治、经济、科技和文化安全，直接危害广大人民群众的利益。

金融财税领域的业务创新为商用密码产品提供了广阔的市场空间。金融、税务、工商、财政等国家关键领域在整个信息产业布局乃至国家战略格局中具有举足轻重的地位，必须采用自主可控的网络信息安全技术为其信息化保驾护航，对网络信息安全有迫切需求，市场潜力巨大。金融财税

领域的各种创新业务，如网上银行、互联网金融、移动支付、网络发票、工商电子营业执照等，迅猛发展，这些创新业务政策性强、涉及面广、影响力大。商用密码产品能够为上述创新业务提供身份认证、数据加密、数字签名等必须的安全功能，具有广阔的市场前景。

网络信息安全产业形态向服务化方向发展。信息系统复杂程度的不断提高和防护难度的不断加大，迫使信息系统用户不得不将网络信息安全服务外包，由此催生一批专业化网络信息安全服务公司。未来，信息安全风险评估、信息系统等级保护咨询、信息系统安全方案设计咨询、信息系统安全集成、信息安全工程监理、信息系统安全运维、网络安全应急处理、数据与系统容灾备份等网络信息安全服务将成为国家重点发展方向，以提高国内企业的网络信息安全服务能力，满足信息化建设对安全可控网络信息安全服务的需求。

安全威胁态势智能感知将成为一个重要方向。各种各样的安全产品被用于检测网络中的攻击威胁，维护网络的安全运行。但这些安全手段一般只能在一定范围内发挥特定的作用，互相之间缺乏有效的数据融合和协同管理机制。面对众多分散的信息，用户无法全面直观地了解系统安全脆弱点、整体攻击状况以及安全防护效果，无法满足预判系统安全脆弱点并提前实施防御措施的需求。此外，随着攻击手段的不断变化，部分高级攻击隐蔽性很强，通过单独的安全产品很

难检测和防护，需要汇总用户网络中所有安全事件信息、威胁信息以及相关数据，结合知识库和网络情报库，快速准确地发现网络异常和高级威胁，同时通过通知用户或与网络中安全设备进行联动，实现针对高级威胁进行智能检测与防护的目的。安全威胁态势感知平台可以有效解决以上问题，其融合了基于大数据的安全分析技术、威胁情报和可视化技术，可以更加系统地分析整体漏洞和风险，呈现整体安全状态，同时能够实现针对攻击风险的预判和预防，并且可以与传统网络安全产品一起联动配合,整体形成网络安全威胁“全局可视、提前预判、主动预警、立体防护”的全新安全解决方案，有效提升安全防护效果和客户体验，因此将成为未来几年安全建设的重要方向。

云计算、物联网安全市场将会成为下一个高速增长点。随着云计算的普及，大量数据和业务都集中在云计算数据中心，云计算数据中心面临着巨大的安全风险，其对安全的需求达到了全新的高度，安全在云计算领域将成为与计算、存储、网络并列的四大基础设施之一，云计算的快速发展给网络安全行业带来了巨大的市场空间和商业价值。近几年来，物联网发展也非常迅猛，物联网技术不仅仅在家庭及消费级设备上取得发展，还在制造业、物流、矿业、石油、公用设施和农业等拥有大型资产的行业开始大量应用。但是物联网的安全性非常薄弱，各类物联网终端很容易成为入侵和控制

的对象，黑客通过入侵物联网设备，逐步渗透到整个网络，窃取大量机密信息，甚至通过操控物联网设备对企业、国家产生直接攻击和威胁。近几年物联网安全事故频发，物联网的安全问题正在被日益重视，后续几年物联网安全市场将会取得快速发展。

整体解决方案能力将变得日益重要。安全产品可分为防火墙、IPS、DDoS 防护、Web 应用防火墙、上网行为管理与审计、漏洞扫描等产品，各类产品配置方法和监控日志形式各异，运维管理非常复杂。随着网络安全的威胁来源和攻击手段不断变化，仅采购和部署几类安全产品无法完全保障网络长期、系统的安全，而对网络进行系统规划、构建全面的安全防护体系、制定完善的安全管理策略、落实日常专业的安全管理显得尤为重要。但是大量中小企业安全技术人员匮乏，并不具备这样的能力，随着网络信息安全环境日益复杂，即使是大型企业和机构也越来越难以独自应对，用户普遍期望安全厂商能够提供全面应对各类安全威胁的整体解决方案，从而降低用户安全管理复杂度。在未来的安全市场中，整体解决方案能力将变得日益重要。