证券代码：688023　　证券简称：安恒信息

杭州安恒信息技术股份有限公司

（杭州市滨江区西兴街道联慧街 188 号）

2020 年度向特定对象发行 A 股股票预案

二〇二〇年十二月

声明

1、本公司董事会及全体董事保证本预案内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性承担个别及连带责任。

2、本次发行完成后，公司经营与收益的变化，由公司自行负责；因本次发行引致的投资风险，由投资者自行负责。

3、本预案是公司董事会对本次向特定对象发行股票的说明，任何与之相反的声明均属不实陈述。

4、投资者如有任何疑问，应咨询自己的股票经纪人、律师、专业会计师或其他专业顾问。

5、本预案所述事项并不代表审批机关对于本次发行相关事项的实质性判断、确认或批准，本预案所述本次发行相关事项的生效和完成尚待取得有关审批、注册机关的批准或核准。

特别提示

1、本次发行方案已经公司于 2020 年 12 月 25 日召开的第一届董事会第二十三次会议审议通过。本次发行方案及相关事项尚需经公司股东大会审议通过、上海证券交易所审核通过及中国证监会同意注册。

2、本次发行对象为不超过 35 名（含 35 名）符合中国证监会规定条件的证券投资基金管理公司、证券公司、信托投资公司、财务公司、保险机构投资者、合格境外机构投资者（QFII）、其它境内法人投资者和自然人等特定投资者。其中，证券投资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象。信托公司作为发行对象，只能以自有资金认购。

最终发行对象由公司董事会或其授权人士根据股东大会授权在本次发行获得中国证监会的注册后，按照中国证监会的相关规定，根据申购报价的情况，遵照价格优先的原则合理确定最终发行对象。

所有发行对象均以同一价格认购本次向特定对象发行的股票，且均以人民币现金方式认购。

3、本次向特定对象发行股票采取询价发行方式，发行价格不低于定价基准日前 20 个交易日公司股票交易均价的 80%（定价基准日前 20 个交易日公司股票交易均价=定价基准日前 20 个交易日公司股票交易总额/定价基准日前 20 个交易日公司股票交易总量），并按照“进一法”保留两位小数。

若公司股票在定价基准日至发行日期间发生派息、送股、转增股本、配股等除权、除息事项，本次发行底价将进行相应调整。

最终发行价格将由股东大会授权董事会在取得中国证监会发行注册文件后，按照中国证监会相关规定，根据竞价结果与本次发行的保荐机构（主承销商）协商确定。

4、本次发行股票的股票数量不超过 22,222,222 股，不超过本次发行前公司总股本的 30%。最终发行数量由公司股东大会授权董事会根据中国证监会相关规定及发行时的实际情况，与本次发行的保荐机构（主承销商）协商确定。若公司

股票在董事会决议日至发行日期间发生送股、资本公积金转增股本、新增或回购注销限制性股票等导致股本总额发生变动的，本次发行的股票数量将进行相应调整。

5、本次发行完成后，发行对象认购的股份自发行结束之日起 6 个月内不得转让。本次发行对象所取得上市公司向特定对象发行股票的股份因上市公司分配股票股利、资本公积金转增等形式所衍生取得的股份亦应遵守上述股份锁定安排。限售期届满后按中国证监会及上海证券交易所的有关规定执行。

6、本次发行募集资金总额不超过 133,332.17 万元，扣除发行费用后，募集资金净额拟投入以下项目：

单位：万元

	项目名称	总投资	募集资金拟投入额
1	数据安全岛平台研发及产业化项目	47,633.85	40,046.62
2	涉网犯罪侦查打击服务平台研发及产业化项目	13,006.66	10,216.18
3	信创产品研发及产业化项目	62,122.22	45,870.82
4	网络安全云靶场及教育产业化项目	15,753.23	12,541.34
5	新一代智能网关产品研发及产业化项目	22,622.09	17,924.13
6	车联网安全研发中心建设项目	10,235.45	6,733.08
	合计	**171,373.50**	**133,332.17**

在上述募集资金投资项目的范围内，公司可根据项目的进度、资金需求等实际情况，对相应募集资金投资项目的投入顺序和具体金额进行适当调整。募集资金到位前，公司可以根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

7、公司一贯重视对投资者的持续回报。根据中国证监会《关于进一步落实上市公司现金分红有关事项的通知》（证监发[2012]37 号）、《上市公司监管指引第 3 号——上市公司现金分红》（证监会公告[2013]43 号）的要求，公司已有完善的股利分配政策，现行有效的《公司章程》对公司的利润分配政策进行了明确的规定。关于公司分红及政策的详细情况请参见本预案“第四节公司利润分配政策和执行情况”。

8、公司提醒投资者关注：本次发行将面临摊薄即期回报的风险。本次发行后公司的净资产和股本将相应增加，由于募集资金投资项目效益的产生需要经历一定时间的项目建设周期，项目产生效益尚需一定的时间。因此，公司净资产收益率和每股收益存在短期内出现下滑情况的可能，未来随着募投项目效益逐步体现，公司的每股收益和净资产收益率将逐步回升。为保障中小投资者的利益，公司就本次发行事项对即期回报摊薄的影响进行了认真分析，并制定填补被摊薄即期回报的具体措施，详见“第五节本次向特定对象发行股票摊薄即期回报分析”。

特此提醒投资者关注本次发行摊薄股东即期回报的风险，公司为应对即期回报被摊薄风险所制定的填补回报措施不等于对公司未来利润做出保证。

9、本次发行符合《公司法》、《证券法》及《上海证券交易所科创板股票上市规则》等法律、法规的有关规定，本次发行完成后，不会导致公司的股权分布不符合上市条件。

目录

释义

除非文中另有所指，下列词语具有如下涵义：

公司、本公司、安恒信息	指	杭州安恒信息技术股份有限公司
本次发行、本次向特定对象发行	指	杭州安恒信息技术股份有限公司向特定对象发行 A 股股票的行为
发行方案	指	杭州安恒信息技术股份有限公司向特定对象发行 A 股股票方案
本预案	指	杭州安恒信息技术股份有限公司 2020 年度向特定对象发行 A 股股票预案
最近三年及一期、报告期	指	2017 年、2018 年、2019 年、2020 年 1-9 月
《公司法》	指	《中华人民共和国公司法》
《证券法》	指	《中华人民共和国证券法》
《公司章程》	指	杭州安恒信息技术股份有限公司章程
股东大会	指	股份公司股东大会
董事会	指	股份公司董事会
监事会	指	股份公司监事会
三会	指	股东大会、董事会、监事会的统称
高级管理人员	指	公司总经理、副总经理 、财务总监、董事会秘书
中国证监会	指	中国证券监督管理委员会
国家发改委	指	中华人民共和国国家发展与改革委员会
工信部	指	中华人民共和国工业和信息化部
上交所	指	上海证券交易所
股票或 A 股股票	指	每股面值为 1.00 元的人民币普通股
绿盟科技	指	北京神州绿盟信息安全科技股份有限公司
启明星辰	指	启明星辰信息技术集团股份有限公司
深信服	指	深信服科技股份有限公司
蓝盾股份	指	蓝盾信息安全技术股份有限公司
北信源	指	北京北信源软件股份有限公司
奇安信	指	奇安信科技集团股份有限公司
阿里云	指	阿里云计算有限公司
赛迪顾问	指	赛迪顾问股份有限公司
GDPR	指	General Data Protection Regulation，通用数据保护条例
WAF	指	Web Application Firewall，网络应用防火墙
URL	指	Uniform Resource Locator，统一资源定位符
IPv4	指	Internet Protocol version 4，互联网协议第四版
IPv6	指	Internet Protocol version 6，互联网协议第六版
漏洞	指	在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，使攻击者能够在未授权的情况下访问或破坏系统

病毒	指	编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码
木马	指	有隐藏性的、自发性的可被用来进行恶意行为的程序
DDoS 攻击	指	分布式拒绝服务（Distributed Denial of Service）攻击，借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动攻击，使计算机或网络无法提供正常的服务
VPN	指	Virtual Private Network，虚拟专用网络
EDR	指	终端检测与响应（Endpoint Detection and Response）,是一种应用机器学习算法与行为分析提供精确、全面、实时的防护与响应的网络安全技术，能够有效发现未知威胁并减少误报
AI	指	Artificial Intelligence，人工智能。它是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学
UEBA	指	用户实体行为分析（User and Entity Behavior Analytics），是一种通过机器学习来发现高级威胁，实现自动化的建模的网络安全技术
沙箱	指	一个虚拟系统程序，允许在沙盘环境中运行浏览器或其他程序，运行所产生的变化可删除
CMMI	指	Capability Maturity Model Integration，即软件成熟度模型集成。由美国卡耐基梅隆大学软件工程学院发布，是一个可以改进系统工程和软件工程的整合模式，能够降低项目的成本，提高项目质量与按期完成率，在世界各地得到了广泛的推广与接受
云计算	指	一种商业计算模型。云计算将计算任务分布在大量计算机构成的资源池上，使各种应用系统能够根据需要获取计算力、存储空间和信息服务
信息安全等级保护	指	对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置
物联网	指	物联网，即基于传感技术的物物相连、人物相连和人人相连的信息实时共享的网络
虚拟化	指	是一种资源管理技术，是将计算机的各种实体资源，如服务器、网络、内存及存储等，予以抽象、转换后呈现出来，打破实体结构间的不可切割的障碍，使用户可以比原本的组态更好的方式来应用这些资源
SaaS	指	Software-as-a-Service，软件即服务
元、万元、亿元	指	人民币元、人民币万元、人民币亿元

除特别说明外，本预案财务数值均保留二位小数，若出现总数与各分项数值之和尾数不符，均为四舍五入原因所致。

第一节　本次向特定对象发行股票方案概要

一、公司的基本情况

公司名称：　杭州安恒信息技术股份有限公司

法定代表人：　范渊

注册资本：　7,407.4075 万元

住所：　浙江省杭州市滨江区西兴街道联慧街 188 号

股票简称：　安恒信息

股票代码：　688023.SH

股票上市地：　上海证券交易所

经营范围：　信息安全设备、网络安全设备、网络安全软件、计算机软硬件、系统集成的技术开发、技术服务，成年人的非证书劳动职业技能培训（涉及前置审批的项目除外），会展服务；生产、加工：信息安全设备、网络安全设备、计算机设备；批发、零售：电子产品、通讯设备、计算机软硬件；货物进出口（法律、行政法规禁止经营的项目除外，法律、行政法规限制经营的项目取得许可证后方可经营）。

二、本次发行的背景和目的

（一）本次发行的背景

1、信息安全上升至国家战略，利好政策助推产业发展

在我国综合实力不断增强，国家发展迎来机遇的同时，国家安全面临着诸多挑战。我国网络安全形势日益多样化、复杂化。在此背景下，信息安全上升至国家战略。2013 年以来，我国先后设立中央国家安全委员会、中央网络安全和信息化委员会，制定并颁布新的《中华人民共和国国家安全法》、《中华人民共和国网络安全法》及相应的配套法规，制定《国家网络空间安全战略》、《“十三五”国家信息化规划》、《软件和信息技术服务业发展规划（2016－2020）》、《信息通信网络与信息安全规划（2016-2020）》等政策，从制度、法规以及政策等维度促进网络安全的不断发展。同时，云计算、大数据、人工智能等新兴技术的加速发

展使得网络安全产品的应用环境日益复杂，数据泄露、高危漏洞等网络安全问题频发，信息安全产品及技术迭代加速，进一步推升网络安全市场需求。

根据中国信通院 2020 年 9 月发布的《中国网络安全产业白皮书》，2019 年我国网络安全产业规模达到 1,563.59 亿元，同比增长 17.1%。根据最新发布的《IDC 全球网络安全支出指南》，2020 年全球网络安全相关硬件、软件、服务市场的总投资将达到 1,252.1 亿美元，较 2019 年同比增长 6.0%；2020-2024 年，IDC 预计年均复合增长率达到 8.1%。IDC 预测，2020 年中国网络安全市场因受到疫情影响总体支出将达到 78.9 亿美元，较 2019 年同比增长 11.0%，与之前预期的 20%以上的增长下滑较大，但依然高于全球平均水平。2021 年开始，IDC 预期行业将恢复到 20%以上的增长，预计 2024 年将达到 167.2 亿美元。我国信息安全建设依然不足，服务和软件的结构上也与全球有较大差距，因此整体行业在政策的不断推动下，总体增长速度较快。

2、数字经济蓬勃发展，安全可信的数据交易成为行业新需求

数字经济蓬勃发展，已成为国民经济中最为核心的增长极之一，我国数字经济增加值规模从 2005 年的 2.6 万亿元扩张到 2019 年的 35.8 万亿元，数字经济占 GDP 比重由 14.2%提升至 36.2%，在国民经济中的地位逐步凸显。党的十八大以来，发展数字经济逐渐上升为国家战略，相关政策文件的出台优化了政策环境。根据中央《关于构建更加完善的要素市场化配置体制机制的意见》，数据资产被明确列入市场生产要素，要求“加快培育数据要素市场”，做到“推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护”。加强信息安全和对个人数据收集的保护已成为国家战略重点。数据价值化进程的加速和数字经济开放合作的深化，对保护数据资源安全提出挑战，新一代数据安全产品需求日益旺盛。

与此相对的，各机构和企业积累的数据信息由于缺乏信息共享平台，形成大量的数据信息孤岛，各方信息不对称，导致数据无法最大化发挥价值。此外，各经济主体在获取数据时，电子数据极易被篡改，篡改行为通过技术手段隐藏，数据真实性无法得到保障。市场对于信息可信环境下共享的需求无法得到有效满足。

3、传统犯罪加速向以互联网为媒介的非接触式犯罪转移，专业涉网犯罪侦查打击支撑工具及技术的需求迫切

我国信息社会快速发展、互联网快速普及使犯罪结构发生了深刻变化，传统接触式犯罪加速向以互联网为媒介的非接触式犯罪转移，目前，我国涉网犯罪呈现出案件持续高发多发、网络诈骗迅猛增长、诈骗窝点快速转移、作案群体逐步泛化、黑灰产业日益泛滥等特点，网络违法犯罪情况错综复杂，侦破难度大大提升。涉网犯罪的日益严峻催生了公安机关采购新型涉网犯罪侦查打击服务的需求。

经过多年的公安信息化建设，我国各级政府及公安部门购买了大量安全软硬硬件产品进行本地化部署。在科技快速发展的时代背景下，安全产品迭代更新加快，导致公安部门安全建设存在投入较大、安全产品重复购买等问题，也对公安网警业务培训提出了更高要求。考虑到该类安全产品本地化部署问题，公安机关采购需求呈现向服务化转变趋势。云计算产业的快速发展，虚拟化及云服务理念的渗透持续加深，也进一步吸引公安机关放弃传统的软硬件产品购置，进行服务采购。未来公安客户将倾向于集中采购安全运营服务，实现一网统办、一网统管，主动、强力、持续的综合性涉网犯罪侦查打击技术服务将成为新需求。

4、国产化替代加速推进，我国信创产业进入快速发展时期

信息技术应用创新产业是国家构建安全可控的自有 IT 产业的重要基础，已经成为经济数字化转型、提升产业链发展的关键。为了解决本质安全问题，大力发展信创产业已上升为一项国家战略。2016 年 4 月 19 日，网信工作座谈会明确提出，“核心技术受制于人是我们最大的隐患”，同年，国家再次强调“抓紧突破网络发展的前沿技术和具有国际竞争力的关键核心技术”。在中美关系动荡之际，信创产业受到了各界的广泛关注，建设安全可控的信息技术体系成为“新基建”和“数字中国”战略的重要内容。2020 年 12 月 16 日至 18 日，中央经济工作会议明确将强化国家战略科技力量和增加产业链供应链自主可控能力列入 2021 年经济工作八大任务。国产化的 IT 底层架构不断完善使得信息技术体系的国产化替代加速推进，我国信创产业进入快速发展时期。

信创产业主要包括新一代信息技术下的云计算、软件（操作系统、中间件、数据库、各类应用软件）、硬件（芯片、GPU/CPU、主机、各类终端）、安全（网

络安全）等领域，涵盖了 IT 底层基础软硬件到上层应用软件的全产业链。随着云计算、大数据、物联网等新技术的发展应用，网络安全应用场景更加复杂，网络攻击组织性与目的性不断加强，社会危害性不断加大。网络安全建设作为信创产业的重要组成部分，自主创新需求更加迫切。

5、网络安全市场快速发展，专业人才缺口扩大，专业教育市场需求旺盛

近几年，随着《网络安全法》的出台，各级政府和企业在网络安全建设方面的投入不断加大。我国网络安全人才需求迅速攀升，截至 2019 年 9 月，我国网络空间安全人才数量缺口高达 70 万，预计到 2020 年将超过 140 万。公司近年业务规模快速增长，网络安全人才需求大幅提升，在不断提高招聘力度的情况下，校招人才缺口仍达 200-300 人。

2016 年 12 月，国家互联网信息办公室印发《国家网络空间安全战略》，提出实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境；2020 年 7 月，全国人大常委会印发《数据安全法（草案）》，再次指出要采取多种方式培养数据开发利用技术和数据安全专业人才。各地政府鼓励网络安全相关学科建设，启动区域网络安全实训基地建设，加强网络安全人才培养成为增强国家网络安全实力的重点，网络安全教育市场空间广阔。

网络安全靶场能够为网络安全人员提供贴近实际生产环境的学习、训练和演练平台，服务于网络安全人才的实战能力养成环节，为网络安全人员的岗位胜任能力培育提供环境和业务形态支撑，随着市场对网络安全人才数量和质量两个维度需求的不断提升，未来网络安全靶场需求也将随之提升。

6、随着新兴技术发展，网关技术进入更新迭代的关键窗口期

随着人工智能、区块链、5G、量子通信、工业互联网、大数据、云计算、物联网等具有颠覆性的战略性新技术快速演进，大规模数据泄露、高危漏洞、新技术应用下的网络攻击等网络安全问题频发，攻击团伙的智能化、商业化生态已形成，网络威胁态势严峻。在云计算、大数据、物联网、工业互联网及 AI 智能防护等新兴技术领域需求的推动下，防火墙作为传统的网关产品处在向智能化、简易化及可视化方向技术更新迭代的关键阶段，现有产品技术架构受到挑战，市

场需要能够满足云计算、大数据、物联网、工业互联网及 AI 智能防护等新兴技术领域安全防护需求的新一代网关产品，行业竞争格局或将面临较大变动，网关技术进入更新迭代的关键窗口期。

7、政策与技术不断完善，车联网及车联网安全发展前景明确

机动车保有量不断上升，导致行车安全和交通拥堵问题日益凸显，而根据美国高速公路安全管理局（NHTSA）提供的统计数据，引入车联网能有效改善现状，中轻型车辆可避免 80%的交通事故，重型车可避免 71%的交通事故，交通拥堵时间可减少 60%，现有道路通行能力提高 2-3 倍。

介于车联网技术优势，国家政策不断鼓励智能网联汽车发展，2019 年 9 月国务院发布《交通强国建设纲要》，明确提出加强智能网联汽车研发，车联网用户渗透率达到 30%以上，联网车载信息服务终端的新车装配率达到 60%以上。在技术方面，5G 与 V2X 技术也加速车联网加速落地。随着 V2X 技术路径的明确，在国家政策和 5G 商用的推动下，基于车联网在驾驶安全性和交通治理方面的突出优势，车联网发展前景进一步明确，目前我国已将车联网产业上升到国家战略高度，我国车联网产业化进程将逐步加快，根据前瞻产业研究院发布的《中国车联网行业市场前瞻与投资战略规划分析报告》统计数据，截至 2017 年，全球车联网市场规模约为 525 亿美元，预计到 2022 年将增加至 1,629 亿美元，复合年均增长率为 25.4%；我国车联网市场规模将从 2017 年的 114 亿美元增长到 2022 年的 530 亿美元，复合年均增长率为 36.0%。随着政策推动与技术发展，车联网行业发展前景明确。

（二）本次发行的目的

1、满足数据安全可信交易的需求，拓展新的市场空间

随着数字经济的发展，网络信息安全作为数字经济发展的必要保障，其投入持续增加，且与全球安全产业结构发展趋势保持一致，我国网络信息安全市场将由软硬件产品逐步向综合安全平台和服务转移。根据赛迪顾问的预测，2019-2021 年度，网络信息安全市场规模的复合增长率为 23.45%，大数据安全市场规模的复合增长率为 35.26%，大数据安全市场规模增速高于网络信息安全行业整体水平，具有较好的市场发展前景。公司于 2015 年起便陆续开发了针对大数据安全

的网络安全态势感知预警平台、AiLPHA 大数据智能安全平台等产品，作为首批切入大数据安全领域的企业，获得了较高的市场占有率，充分享有大数据安全市场规模增长所带来的红利，2017-2019 年度公司网络信息安全平台中大数据安全产品相关收入年复合增长率达到 100.22%。

通过本次数据安全岛平台研发及产业化项目的实施，公司能够更充分利用自身在大数据安全领域的技术积累，解决大量的数据信息孤岛、信息不对称问题，把握数字经济快速发展带动的数据交易平台及其有关技术服务需求增长，实现对公司网络信息安全平台产品系列的拓展与补充，进一步提升公司网络信息安全平台业务，进而提高公司整体盈利能力。

2、顺应公安客户对涉网犯罪打击工具的新需求，促进客户涉网犯罪打击能力提升

本次发行募集资金用于研发落地涉网犯罪侦查打击服务平台，平台基于浦东公安实际业务场景，利用大数据技术，开展犯罪行为监测预警、犯罪线索智能落地、辅助案件研判、犯罪业态感知、本地产业评价等业务，顺应客户对于 SaaS 化涉网犯罪打击工具的新需求，增加客户粘性提升公司盈利能力，同时促进客户涉网犯罪打击能力的迅速提升，有利于提高我国网络安全综合治理能力和水平，推进构建安全清朗、和谐稳定的网络空间。

3、顺应国产化替代趋势，把握信创领域网络安全市场发展机遇

随着国产 CPU、操作系统等基础层产品不断完善，安全自主可控的信息化建设进程的推进，下游客户对信创网络安全产品和服务需求强烈，行业市场空间广阔。信创产业的不断发展下，国产化替代已从电信运营商、政府、金融等关键敏感行业逐步向全行业展开。

面对国产化替代明确的发展趋势，公司拟依托在网络安全领域的产品技术和人才基础，依据国家战略要求，对基础网络安全产品、云安全管控平台、态势感知平台和安全运营平台等进行国产化适配。基于国产化平台，全面开展信创领域的安全咨询、安全集成、安全运营等工作，加强对运维访问控制审计技术、分布式漏洞发现与验证技术、基于云架构的安全扫描与监测技术、SaaS 化云安全防护等技术的研发力度。本次信创产品研发及产业化项目是公司顺应国产替代安全

可控大趋势，满足软件技术可控集采要求的必然选择，是公司保持并提升主要下游市场竞争力的重要战略。

4、提高网络安全教育培训能力，抢占市场份额

本次网络安全云靶场及教育产业化项目基于网络安全行业人才紧缺的现状，以及当前学历教育与职业技能水平不匹配的问题，搭建网络安全靶场，为网络安全人才培养提供了环境、专业工具和业务形态支撑，有助于解决高层次专业教师缺乏，教材良莠不齐，缺乏攻防演练平台，综合性、自主防御性试验难以构建和学生缺少实战等问题。通过网络安全靶场平台产品研发，加强现有网络安全产品向适用于教育教学产品的转化研发，为我国网络安全教学内容建设和网络安全人才培养提供实战化培训工具，有利于丰富我国网络安全人才培养模式，提高网络安全人才培养能力和水平，进而满足日益增长的网络安全人才需求。

同时该项目的建设实施有助于扩展公司网络安全教学类产品市场空间，实现以实战为导向的网络安全培训服务，对网络安全人才培养产品和服务进行一体化升级，从横向上扩展公司业务线。另一方面，公司为学校、大型企业和政府建设网络安全靶场提供相应的产品，有助于加强潜在用户对公司产品的认知，推广相关网络安全产品，推进公司生态建设。项目将更好地满足国家培育行业人才战略的需要，同时拓展新的产品业务领域，在推动公司业绩增长的同时，进一步提升行业整体竞争力。

5、抓住网关行业技术迭代机遇，扩大公司相关产品市场规模

伴随国家网络强国战略和企业数字化转型的推进，云计算、大数据、人工智能等新兴技术的加速发展使得网络安全产品的应用环境日益复杂，迫使新一代网络安全产品综合协作能力快速提升，新一代网关产品进入技术更新迭代的关键窗口期，推动传统网关产品技术淘汰。目前，公司业务主要集中在应用层安全领域，基础层安全产品市场份额较小。本次新一代智能网关产品研发及产业化旨在把握行业技术迭代窗口期，对新一代智能网关产品进行研发升级，完善公司网关产品核心技术，适应新的应用环境和技术方向，提升公司在云计算、大数据、物联网、工业互联网及人工智能等新兴技术领域综合安全解决方案的完整性和适配性，抓住机遇抢占市场份额，进一步扩大公司产品业务规模，提升整体竞争力。

6、把握车联网明确的发展前景，拓展产品市场空间

公司拟通过身份认证体系、车辆安全检测、靶场虚拟化技术、威胁情报获取和车载微流量技术的研发，凭借公司在网络信息安全领域成熟的产品技术将传统安全产品技术向车联网场景研发转化，形成完善的车联网安全产品体系，满足车联网网络安全需求，推动车联网产业链的建设完善。通过开展车联网安全关键技术研发和储备，为公司未来拓展车联网安全业务提前进行产品技术布局，抓住车联网明确的发展前景以拓展网络安全产品的市场空间。

7、增强资金实力，为公司战略布局提供充分保障

通过本次向特定对象发行 A 股股票募集资金，将进一步增强公司资金实力，优化资产负债结构，提高公司抗风险能力。同时，本次向特定对象发行股票募集资金均用于公司的主营业务，募投项目与现有业务关联度高，是加强公司对前沿技术的研发、支撑行业应用的持续升级、深化公司在网络安全行业相关领域业务布局的重要举措。待本次募集资金投资投产后，公司将实现业务板块的延伸和扩展，随着募投项目的实施及效益的产生，公司的盈利能力和经营业绩将进一步提升。

三、本次向特定对象发行股票方案概要

（一）本次发行股票的种类和面值

本次发行股票的种类为境内上市人民币普通股（A 股），每股面值人民币 1.00 元。

（二）发行方式和发行时间

本次发行的股票全部采取向特定对象发行的方式，将在中国证监会同意注册后的有效期内选择适当时机向特定对象发行。

（三）发行对象及认购方式

本次发行对象为不超过 35 名（含 35 名）符合中国证监会规定条件的证券投资基金管理公司、证券公司、信托投资公司、财务公司、保险机构投资者、合格境外机构投资者（QFII）、其它境内法人投资者和自然人等特定投资者。证券投

资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托投资公司作为发行对象的，只能以自有资金认购。

最终发行对象将在本次发行经上海证券交易所审核通过并经中国证监会同意注册后，由公司董事会根据询价结果，与保荐机构（主承销商）协商确定。若发行时法律、法规或规范性文件对发行对象另有规定的，从其规定。

所有发行对象均以人民币现金方式并以同一价格认购公司本次发行的股票。

（四）发行数量

本次向特定对象发行股票的股票数量不超过 22,222,222 股，本次发行的股票数量按照本次发行募集资金总额除以发行价格计算，不超过本次发行前公司总股本的 30%。最终发行数量由公司股东大会授权董事会根据中国证监会相关规定及发行时的实际情况，与本次发行的保荐机构（主承销商）协商确定。

若本公司股票在董事会决议日至发行日期间发生送股、资本公积金转增股本、新增或回购注销限制性股票等导致股本总额发生变动的，本次向特定对象发行股票的数量将进行相应调整。

若本次向特定对象发行的股份总数因监管政策变化或根据发行注册文件的要求予以变化或调减的，则本次向特定对象发行的股份总数及募集资金总额届时将相应变化或调减。

（五）定价基准日、发行价格及定价原则

本次发行的定价基准日为公司本次向特定对象发行股票的发行期首日。

本次向特定对象发行股票采取询价发行方式，发行价格不低于定价基准日前 20 个交易日公司股票交易均价的 80%（定价基准日前 20 个交易日公司股票交易均价=定价基准日前 20 个交易日公司股票交易总额/定价基准日前 20 个交易日公司股票交易总量），并按照“进一法”保留两位小数。

最终发行价格将在公司取得中国证监会对本次发行予以注册的决定后，由股东大会授权公司董事会或董事会授权人士和保荐机构（主承销商）按照相关法律法规的规定和监管部门的要求，遵照价格优先等原则，根据发行对象申购报价情

况协商确定。

若公司股票在本次发行的定价基准日至发行日期间发生派发股利、送红股、公积金转增股本等除权除息事项，本次发行底价将作相应调整。调整方式如下：

派发现金股利：P1=P0-D

送红股或转增股本：P1=P0/（1+N）

派发现金同时送红股或转增股本：P1=（P0-D）/（1+N）

其中，P0 为调整前发行底价，D 为每股派发现金股利，N 为每股送红股或转增股本数量，调整后发行底价为 P1。

（六）锁定期安排

本次发行完成后，发行对象认购的股份自发行结束之日起六个月内不得转让。法律法规、规范性文件对限售期另有规定的，依其规定。

本次向特定对象发行股票结束后，由于公司送红股、资本公积金转增股本等原因增加的公司股份，亦应遵守上述限售期安排。

本次发行的发行对象因本次发行取得的公司股份在锁定期届满后减持还需遵守《公司法》《证券法》《上市规则》等法律法规、规章、规范性文件、交易所相关规则以及公司《公司章程》的相关规定。

（七）募集资金数量及用途

本次向特定对象发行股票募集资金总额不超过 133,332.17 万元，扣除发行费用后，募集资金净额拟投入以下项目：

单位：万元

	项目名称	总投资	募集资金拟使用额
1	数据安全岛平台研发及产业化项目	47,633.85	40,046.62
2	涉网犯罪侦查打击服务平台研发及产业化项目	13,006.66	10,216.18
3	信创产品研发及产业化项目	62,122.22	45,870.82
4	网络安全云靶场及教育产业化项目	15,753.23	12,541.34
5	新一代智能网关产品研发及产业化项目	22,622.09	17,924.13
6	车联网安全研发中心建设项目	10,235.45	6,733.08

	合计	**171,373.50**	**133,332.17**

在上述募集资金投资项目的范围内，公司可根据项目的进度、资金需求等实际情况，对相应募集资金投资项目的投入顺序和具体金额进行适当调整，募集资金到位前，公司可以根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

（八）上市地点

本次发行的股票拟在上海证券交易所科创板上市交易。

（九）滚存未分配利润的安排

公司本次发行前的滚存未分配利润由本次发行完成后公司的新老股东按照发行后的持股比例共同享有。

（十）本次发行的决议有效期

本次发行的决议自公司股东大会审议通过本次发行方案之日起12个月内有效。若国家法律、法规对向特定对象发行股票有新的规定，公司将按新的规定进行相应调整。

四、本次发行是否构成关联交易

截至本预案公告日，本次发行尚未确定发行对象，最终是否存在因关联方认购公司本次向特定对象发行股票构成关联交易的情形，将在发行结束后公告的发行情况报告书中予以披露。

五、本次发行是否导致公司控制权发生变化

本次发行前，公司的控股股东、实际控制人为范渊，其直接持有公司 10,018,362 股股份，占公司总股本的 13.52%，并通过和员工持股平台嘉兴安恒、宁波安恒的《一致行动协议》，合计控制安恒信息 27.02%的表决权。

本次向特定对象拟发行不超过本次发行前公司总股本的 30%，即不超过 22,222,222 股(含本数)，本次发行完成后公司的总股本不超过 96,296,297 股(含本

数)。按发行 22,222,222 股上限测算，本次发行完成后，控股股东及实际控制人范渊可实际控制的表决权约占公司总股本的 20.79%，仍保持实际控制人的地位。本次发行不会导致公司控股股东和实际控制人发生变更。

六、本次向特定对象发行股票的审批程序

本次向特定对象发行的方案及相关事项已经于 2020 年 12 月 25 日召开的公司第一届董事会第二十三次会议审议通过，尚需履行以下审批：

1、本次向特定对象发行股票尚需取得本公司股东大会审议通过；

2、本次向特定对象发行股票尚需取得上海证券交易所审议通过；

3、本次向特定对象发行股票尚需获得中国证监会注册同意。

七、本次发行是否导致股权分布不具备上市条件

本次发行不会导致公司股权分布不具备上市条件。

第二节　董事会关于本次募集资金使用的可行性分析

一、本次募集资金使用计划

本次向特定对象发行股票募集资金总额不超过 133,332.17 万元，扣除发行费用后，募集资金净额拟投入以下项目：

单位：万元

	项目名称	总投资	募集资金拟使用额
1	数据安全岛平台研发及产业化项目	47,633.85	40,046.62
2	涉网犯罪侦查打击服务平台研发及产业化项目	13,006.66	10,216.18
3	信创产品研发及产业化项目	62,122.22	45,870.82
4	网络安全云靶场及教育产业化项目	15,753.23	12,541.34
5	新一代智能网关产品研发及产业化项目	22,622.09	17,924.13
6	车联网安全研发中心建设项目	10,235.45	6,733.08
	合计	**171,373.50**	**133,332.17**

在上述募集资金投资项目的范围内，公司可根据项目的进度、资金需求等实际情况，对相应募集资金投资项目的投入顺序和具体金额进行适当调整。募集资金到位前，公司可以根据募集资金投资项目的实际情况，以自筹资金先行投入，并在募集资金到位后予以置换。募集资金到位后，若扣除发行费用后的实际募集资金净额少于拟投入募集资金总额，不足部分由公司以自筹资金解决。

二、本次募集资金投资项目可行性分析

（一）数据安全岛平台研发及产业化项目

1、项目概况

数据流动是带动数据分析、挖掘和利用，最大化释放数据价值的基础，根据中央《关于构建更加完善的要素市场化配置体制机制的意见》，数据资产被明确列入市场生产要素，要求“加快培育数据要素市场”，做到“推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护”。加强信息安全和对个人数据收集的保护已成为国家战略重点。2018 年 8 月，十三届全国人大常委会将《数据安全法》、《个人信息保护法》纳入一类立法计划，数据安全领域立法进入快车道，将进一步规范各方在数据保护中的义务与责任。《中华人民

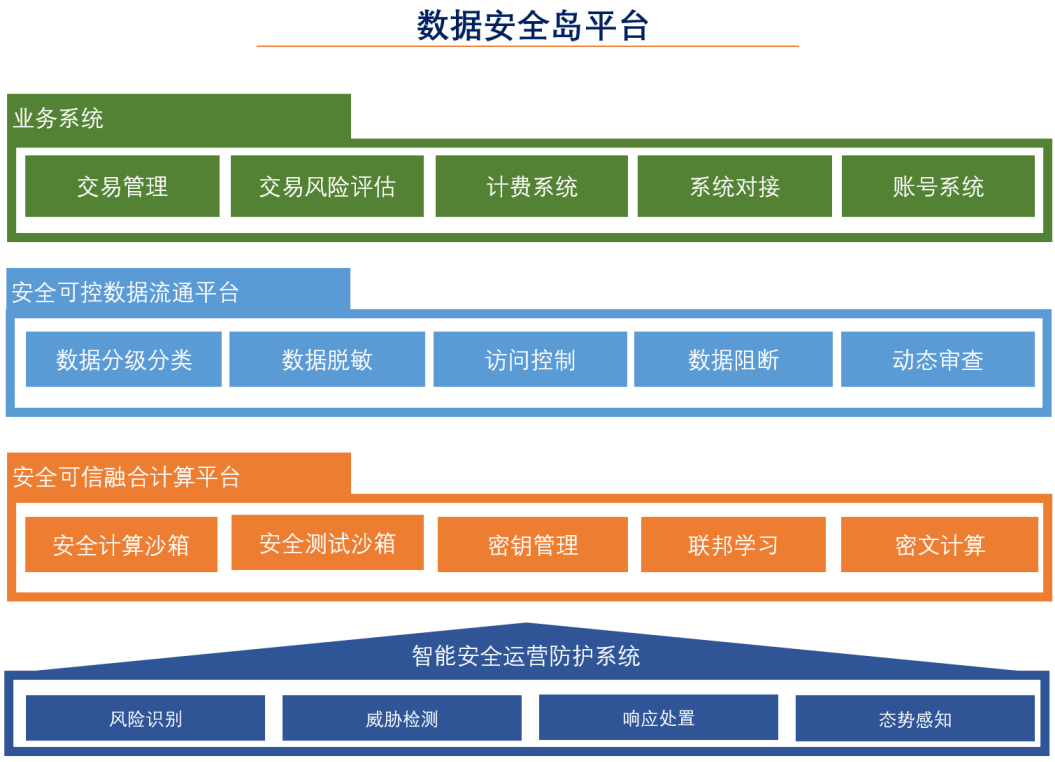
共和国数据安全法（草案）》提出国家支持建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。立法工作的推进和重点领域个人信息保护执法力度的强化使得数据交易和共享的安全保障需求快速增长。

国内目前的数据交易市场所采用的供应方直接将数据传输给购买方的方式，缺乏第三方平台介入提供脱敏等服务，需要供应方耗费大量精力处理原始数据中的敏感信息，数据交易效率低下。同时，该方式也存在数据交换认证机制不完善、审计及防护缺失等问题，导致数据交易过程中出现泄露倒卖数据、篡改数据并流出等问题，为数据供应方带来较大法律风险，降低其交易意愿，不利于数据的充分流通。

鉴于市场日趋强烈的数据交易需求及合理可信的数据交易方式与专业安全数据流通平台的缺失，公司拟依托上海临港区位优势，在上海临港新片区购置土地，建设数据安全研发基地，重点开展数据交易安全平台即安全岛产品的研发及产业化，改善当前数据交易困境。数据安全岛通过数据全链路加密、操作留痕、各主体数据隔离、密文计算、异常情况动态分析等技术手段，规避数据泄露、篡改等风险，同时还可以提供数据自动脱敏服务提高数据流转效率。

2、项目建设内容

数据安全岛平台主要由业务系统、安全可控数据流通平台、安全可信融合计算平台和智能安全运营防护系统构成，平台架构图及各模块主要功能如下：



①业务系统：包括交易管理、交易风险评估、计费系统、系统对接和账号系统功能。

交易管理通过对数据所有权和使用权分离，提供安全、便捷和灵活的数据使用权让渡交易管理服务；

交易风险评估可提供数据交易的事前合规评估功能，保障数据交易合规管理要求；

计费系统、系统对接和账号系统则为系统使用者提供计费、与外部系统对接和账号管理等功能。

②安全可控数据流通平台：包括数据分级分类、数据脱敏、数据阻断、访问控制和动态审查功能。

数据分级分类通过遵循国家和各行业分级分类规范，研发数据分级分类引擎；

数据脱敏通过敏感数据识别字典和脱敏算法处理数据中的敏感信息，实现敏感信息保障脱敏后数据的一致性和业务关联性；

数据阻断运用 AI 智能研判分析技术，通过对流动数据的监听，发现违规及时阻断，保障数据流通的安全可控；

访问控制通过 UBA（用户行为分析）技术实现对用户行为和用户身份持续风险监测，动态调整用户权限，拦截超身份认证的数据访问行为；

动态审查通过基于区块链的交易状态跟踪和大数据分析，提供数据交易的事中安全审计及事后数据溯源功能。

③安全可信融合计算平台：提供多方数据融合计算解决方案，包括安全计算沙箱、安全测试沙箱、密钥管理和数据仓库功能。

安全计算沙箱通过为每个计算任务创建独立的容器环境，实现不同合约在静态储存状态与执行计算状态下都保持数据之间的完全隔离。安全计算沙箱内的计算任务和操作均经审计和记录，实现操作监控和后续事件溯源；

安全测试沙箱是为开发人员提供的测试环境，通过开放部分样本数据进行算法调试，确保数据在安全计算沙箱的算法准确性；

密钥管理支持独立密钥管理体系，包含加密密钥生成、分配、备份和恢复四部分，加密密钥统一由主密钥保护，主密钥则通过硬件密码设备产生并管理，确保密钥安全；

联邦学习通过在本地进行模型训练，然后仅将模型参数加密上传到数据交换区域，并与其他各方训练模型参数进行聚合，以达到原始数据不出本地，模型训练效果最佳的结果；

密文计算可以实现数据加密状态下的多方数据安全计算。

④智能安全运营防护系统：包括风险识别、威胁检测、响应处置和态势感知功能。

风险识别基于漏洞和配置核查信息，结合数据库系统、网络系统、应用系统等数据，识别网络环境内风险信息；

威胁检测通过 UEBA、威胁情报、ATT&CK 等技术，实现对网络攻击、漏洞利用、横向扩散、用户异常行为、数据泄露等风险的检测和分析；

响应处置基于风险识别和威胁检测的结果，利用 SOAR 技术，对响应流程自动化编排，实现从静态事件响应到动态工作流跟踪的转变，提升整体的协调及决策能力；

态势感知能力主要在全局监测数据、智能分析数据等多维数据的态势分析之上，形成综合态势、攻击态势、威胁态势、预警态势等多种态势感知能力。

本项目中数据安全岛平台的研发涉及数据智能分类分级技术、数据动态脱敏技术、安全计算沙箱技术、多方数据联合建模技术、数据主动销毁技术、用户实体行为分析（UEBA）技术、动态数据网关技术等，相关技术主要研发内容及在产品中的应用如下：

技术方向	主要研发内容	相关技术在产品中的应用
数据智能分类分级技术	数据测绘、数据分级分类引擎等技术研究	在数据安全岛平台中对纳入共享交换的数据，需要根据国家、行业和地方法规进行分级分类，并根据结果进行针对性开放共享。
数据动态脱敏技术	敏感数据识别、数据动态脱敏等技术研究	在数据安全岛平台中对需要对开放的数据进行脱敏处理，避免敏感信息泄露，保障脱敏后数据的一致性和业务关联性。
安全计算沙箱技术	数据隔离、可信执行环境 TEE、操作监控和历史行为回放等技术研究	在数据安全岛平台的安全可信计算场景中，利用安全计算沙箱，解决多方数据融合计算过程中遇到的任务干扰、数据干扰以及数据可能被窃取的风险，用户可基于大数据环境提交算法、程序和学习模型执行分析，可实现基于数据共享需求的安全、自由建模能力。
多方数据联合建模技术	差分隐私、联邦学习、同态加密等技术研究	在数据安全岛平台中需要实现跨组织多方数据的联合建模应用，实现“数据出域”和“数据不出域”两种联合建模方式，解决多方数据联合建模过程的信任难题。
数据主动销毁技术	数据级联销毁、区块链等技术研究	在数据安全岛平台的安全计算沙箱，需具备计算任务完成后，主动销毁沙箱内的明文数据，并利用区块链技术保存沙箱审计日志，保障数据主动销毁的可信度。
用户实体行为分析（UEBA）技术	用户行为数据治理、用户特征工程、用户异常归一化映射评分等技术研究	在数据安全岛平台的账户行为动态鉴权场景中，实现在数据的使用过程中，动态分析账户行为是否异常，识别可能会造成数据泄露风险的高危人员，保障数据不被攻击者利用伪装身份使用。
动态数据网关技术	代码语法分析解析、环境识别、SOAR（安全编排、自动化及响应）等技术研究	结合 UEBA 技术的分析结果，利用 SOAR 和动态阻断策略，对非法行为的动态阻断，以此保障数据的动态安全。

3、项目必要性

（1）我国数字经济蓬勃发展，数据安全产品需求日益旺盛

数字经济蓬勃发展，已成为国民经济中最为核心的增长极之一，我国数字经济增加值规模从 2005 年的 2.6 万亿元扩张到 2019 年的 35.8 万亿元，数字经济占 GDP 比重由 14.2%提升至 36.2%，在国民经济中的地位逐步凸显。党的十八大以来，发展数字经济逐渐上升为国家战略，相关政策文件的出台优化了政策环境，2020 年初政府加速布局“新基建”为数字经济发展提供了新动能。数据价值化进程的加速和数字经济开放合作的深化，对保护数据资源安全提出挑战，新一代数据安全产品需求日益旺盛。

与此相对的，各机构和企业积累的数据信息由于缺乏信息共享平台，形成大量的数据信息孤岛，各方信息不对称，导致数据无法最大化发挥价值。此外，各经济主体在获取数据时，电子数据极易被窃取，窃取行为通过技术手段隐藏，数据流动过程中安全性无法得到保障。

为抓住时代发展机遇，公司拟基于在数据安全领域的技术积累开发数据安全岛平台解决方案，为数据交易和共享平台提供技术支持服务。本项目实施将为数字经济发展提供安全可靠的数据交易平台，可供多方数据联合计算，有利于打破数据孤岛，实现数据流通，创造数据价值。公司针对政府和企业客户日益强烈的数据交易和共享需求设计的数据安全岛平台能够为我国数字经济发展提供所需的安全保障。

（2）本项目能够满足客户数据安全合规及降低数据泄露风险需求，拓展新的市场空间

近年来大数据行业在蓬勃发展的同时也滋生了大量数据黑灰产，非法收集、使用数据给数据拥有方造成了高昂的经济损失。根据 IBM 发布的《2020 年数据泄露成本报告》[1]，2019 年 8 月至 2020 年 4 月期间全球范围内发生了 524 起大型数据泄露违规事件，涉及 17 个地区和 17 个行业的各种规模的组织，平均每件数据泄露事件会造成 386 万美元的经济损失，受害者组织发现和控制数据泄露平均

[1]《2020 年数据泄露成本报告》
https://securityaffairs.co/wordpress/106710/reports/2020-cost-of-a-data-breach-report.html

需要 280 天。根据报告，客户个人身份信息（PII）记录每条丢失或被盗的平均成本为 150 美元，知识产权记录平均每条丢失成本为 147 美元，员工信息丢失成本为 141 美元，全球范围内 80%的数据泄露都导致了丢失成本最为高昂的客户 PII 丢失。

加强信息安全，保护个人数据隐私不仅是各类组织经济层面的需求，更是企业满足合规性产生的法律层面的需求。数据安全领域立法已经进入了快车道，2018 年 8 月十三届全国人大常委会将《数据安全法》、《个人信息保护法》纳入一类立法计划，2020 年 7 月《数据安全法（草案）》公布，提出国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。同时，《草案》明确了数据安全制度和保护义务，列明任何组织、个人收集数据，必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。在数字经济发展带动数据流动需求快速增长和个人信息保护法律法规等政策环境逐步完善的背景下，对数据交易平台及平台的安全可信技术保障能力提出要求。

为了推动在合法合规条件下个人信息数据的收集和使用，各地政府等相关客户对数据安全交易和共享平台的建设需求快速涌现，公司拟充分利用区块链的去中心化、溯源、防篡改等特性，结合数据主动销毁、数据操纵行为监控、账户风险动态感知等技术，实现一个跨机构、跨地域的，集数据订阅、交换、联合计算等功能的可信平台，同时赋予平台脱敏等功能，实现交易自动化降低人力成本，发挥数据的最大价值，实现数据交易过程中的数据安全和个人信息保护，顺应客户新需求，拓展新的市场空间。

（3）本项目是公司把握新的市场机遇，进一步提升网络信息安全平台业务的重要举措

随着数字经济的发展，网络信息安全作为数字经济发展的必要保障，其投入持续增加，且与全球安全产业结构发展趋势保持一致，我国网络信息安全市场将由软硬件产品逐步向综合安全平台和服务转移。根据赛迪顾问的预测，2019-2021 年度，网络信息安全市场规模的复合增长率为 23.45%，大数据安全市场规模的复合增长率为 35.26%，大数据安全市场规模增速高于网络信息安全行业整体水平，具有较好的市场发展前景。公司于 2015 年起便陆续开发了针对大数据安全的网络安全态势感知预警平台、AiLPHA 大数据智能安全平台等产品，作为首批

切入大数据安全领域的企业，获得了较高的市场占有率，充分享有大数据安全市场规模增长所带来的红利，2017-2019 年度公司网络信息安全平台中大数据安全产品相关收入年复合增长率达到 100.22%。

通过本项目的实施，公司能够更充分利用自身在大数据安全领域的技术积累，把握数字经济快速发展带动的数据交易平台及其有关技术服务需求增长，研发数据安全岛平台，实现对公司网络信息安全平台产品系列的拓展与补充，进一步提升公司网络信息安全平台业务，提升公司整体盈利能力。

（4）打造临港数据交流安全可信平台有助于树立数据交易平台的建设标杆，助推公司产品市场拓展

2019 年 8 月，国务院印发《中国（上海）自由贸易试验区临港新片区总体方案》，提出实施国际互联网数据跨境安全有序流动，包括构建安全便利的国际互联网数据专用通道，支持新片区聚焦集成电路、人工智能、生物医药、总部经济等关键领域，试点开展数据跨境流动的安全评估，建立数据保护能力认证、数据流通备份审查、跨境数据流通和交易风险评估等数据安全管理机制。

基于临港数据流动和交易平台建设需求，本项目拟在上海临港新片区购置土地，重点开展数据安全岛平台研发，为政府等相关部门搭建可服务于国内外数据交流的安全可信平台提供完整的安全可信保障产品技术方案。本项目有助于树立行业内数据交易平台的建设标杆，迅速建立公司产品在该领域的知名度和市场地位，确立竞争优势，保障未来业绩实现。

4、项目可行性

（1）国家数据安全领域政策的发布规范了行业标准，利于项目落地与推广

从欧盟、美国等发达地区与国家的发展经验来看，数据流通与交易市场的发展离不开相关法规的落地，法规为行业技术提供了统一的行动规范与衡量准则，利于相关产品各参与方高效地联系与衔接，生产出标准化的软件工程产品。如 GDPR 准则规范了欧盟所有成员国数据的收集、传输、保留或处理行为，因此任何一个欧盟国家研发的相关产品均可以向联盟全体参与国推广。

目前我国数据安全、个人信息保护领域的立法已在有序开展，数据安全交易行业标准的出台指日可待。2018 年 8 月，十三届全国人大常委会将《数据安全法》、《个人信息保护法》纳入一类立法计划，之后陆续发布了《互联网个人信息安全保护指南》、《个人信息出境安全评估办法（征求意见稿）》、《儿童个人信息网络保护规定》和《App 违法违规收集使用个人信息行为认定方法》等对数据安全和个人信息安全进行保护。2020 年 7 月，《中华人民共和国数据安全法（草案）》公布，对数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开发和法律责任进行了明确。

数据安全和个人信息保护领域一系列政策的发布有利于规范行业内的数据收集、交易和开发利用，为该领域数据安全产品技术和保障能力建设提供了切实可行的通用标准。同时，数据安全立法提升了企业对于数据安全的法律风险责任，进一步催生了数据交易平台及安全可信技术需求,为本项目提供了政策保障。

（2）数字经济快速发展和数据价值化推进为本项目提供了市场保障

近年来我国数字经济蓬勃发展，对 GDP 的贡献水平显著提升，2014 年到 2019 年我国数字经济对 GDP 增长始终保持在 50%以上的贡献率，2019 年数字经济对经济增长的贡献率为 67.7%，成为驱动我国经济增长的核心关键力量。在中央《关于构建更加完善的要素市场化配置体制机制的意见》中，数据资产被明确列入市场生产要素，要求“加快培育数据要素市场”，做到“推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护”。随着数字产业化的稳步增长、产业数字化的深入推进，以及我国数字化治理能力的不断提升，未来加速数据要素价值化进程、深化数字经济开放合作将是我国数字经济发展的重点方向。

在数字经济发展和数据价值化推进的过程中，政府和企业对数据交易和共享的需求快速增长，带动数据交易平台及其有关技术服务的市场增长，为本项目的顺利实施提供了市场保障。

（3）公司丰富的技术积累和人才储备为本项目提供技术保障

数据安全岛平台是对多种网络安全前沿技术的集成与融合，涉及数据隔离、可信环境执行、安全计算沙箱、用户实体行为分析以及多方数据联合建模等技术。

公司自设立以来始终坚持持续技术创新的发展战略，重视研发投入，过去三年研发费用占营业收入比例均超过 20%，截至 2020 年 9 月 30 日，公司共拥有 48 项核心技术，研发人员数量达 869 人，涉及攻防研究、应急响应、安全咨询、漏洞研究、产品研发等各个领域。良好的研发创新能力、完善的技术体系和强大的人才团队为本项目的顺利实施提供了技术保障。公司已完成本项目产品核心安全计算沙箱技术和多方数据联合建模技术应用框架研究，进入技术应用测试和优化开发阶段。目前已有一项相关专利获得授权，另有多项技术发明专利进入申请受理状态与实审状态。

（4）临港区位优势为本项目提供了便利条件

临港作为开放程度极高的自由贸易园区，园区内有大量存在数据交流需求的企业，且国家层面也对临港园区的数据流动能力提出了期望。根据国务院印发的《中国（上海）自由贸易试验区临港新片区总体方案》，提出临港自由贸易区要对标国际上公认的竞争力最强的自由贸易园区，选择国家战略需要、国际市场需求大、对开放度要求高的重点领域，实施具有较强国际市场竞争力的开放政策和制度。2019 年 8 月 20 日，中国（上海）自由贸易试验区临港新片区揭牌，当年实现新设企业 4,025 家，签约重点项目 168 个、总投资 821.9 亿元[2]。2020 年 1 月 2 日，临港新片区荣获商务部“国家外贸转型升级基地（汽车及零部件）”和上海市商务委“上海国际服务贸易示范基地”授牌，将进一步突出新片区在信息、要素和资源集聚的优势，在数字贸易、技术贸易和服务外包等领域加快推进新片区服务贸易发展。临港的区位优势为本项目的顺利实施提供了便利。

5、投资概算

本项目预计建设期为 3 年，项目总投资 47,633.85 万元，拟投入募集资金 40,046.62 万元，其余所需资金通过自筹解决。项目具体投资情况如下：

单位：万元

序号	项目名称	投资总额	募集资金金

[2]数据来源：2019 年政府信息公开工作年度报告（中国（上海）自由贸易试验区临港新片区管理委员会）http://www.lgxc.gov.cn/contents/27/24601.html

			额
1	**工程建设费用**	**33,583.35**	**33,583.35**
1.1	土地款	2,860.40	2,860.40
1.2	场地建造费	26,742.75	26,742.75
1.3	硬件购置	2,815.60	2,815.60
1.4	软件购置	1,164.60	1,164.60
2	**研发费用**	**10,353.75**	**6,463.27**
3	**基本预备费 2%**	**878.74**	**-**
4	**铺底流动资金**	**2,818.01**	**-**
	合计	**47,633.85**	**40,046.62**

6、实施主体、项目选址和建设期限

本项目实施主体为公司间接全资控股子公司上海安恒互联安全科技有限公司。公司拟依托上海临港区位优势，在上海临港新片区购置土地，重点开展数据交易安全平台即安全岛产品研发及产业化，预计建设期为 3 年。上述项目建设所需土地将于近期完成土地招拍挂程序。

7、项目备案和环评情况

截至本预案出具日，本项目的可行性研究报告已编制完毕，公司正在办理备案等相关事项。

8、项目经济效益评价

经测算，本项目税后内部收益率为 22.00%，税后静态投资回收期为 7.03 年，项目预期效益良好。

（二）涉网犯罪侦查打击服务平台研发及产业化项目

1、项目概况

以大数据、区块链、人工智能为技术引导的新一代互联网技术快速发展的同时也带来了涉网犯罪案件数量快速增长。该类犯罪手法更新升级迅速，且具有虚拟性、隐蔽性、瞬时性、团伙化、低龄化等特点，作案涉及面广、社会危害重，给公安机关发现和打击违法犯罪带来了新的挑战。自 2018 年开始，公安部连续开展了“净网 2018”和“净网 2019”专项行动，严厉打击侵犯公民个人信息、黑客攻击破坏、网络诈骗、网络水军、网络赌博、网络色情、网约犯罪等突出违法犯罪行为。在此高压态势之下，犯罪产业逐步向规模化、标准化、精细化转型，

公安部门的打击难度和成本大幅提高，要求公安部门整合资源手段、创新机制方法，加强涉网犯罪打击和治理能力，公安系统对专业涉网犯罪侦查打击支撑工具及技术的需求日益显现。

本项目拟在上海浦东新区租赁办公场地，研发落地涉网犯罪侦查打击服务平台，开展定制化侦查破案及案件线索检索平台等业务。平台利用大数据技术，开展犯罪行为监测预警、犯罪线索智能落地、辅助案件研判、犯罪业态感知、本地产业评价等业务，为公安客户提供涉网犯罪情报发现和线索分析等远程 SaaS 化服务，协助公安客户提高涉网犯罪侦查打击能力。

2、项目建设内容

涉网犯罪侦查打击服务平台主要由数据采集和数据分析两大模块构成，平台架构及各模块主要功能如下：

①数据采集模块：通过分布式网络空间测绘引擎对相关网站的关键内容进行实时监测，建立互联网开源数据和互联网通信基础数据资源库，并对其进行加工整理，形成基础的域名库、IP 库、DNS 库、企业信息库、网站信息库、APP 信息库等专题库。

②数据分析模块：由多种分析算法和算法运行环境组成。算法系根据以往公安干警案件、安恒技术专家协助侦查的工作积累开发出来的自动化的通用分析方法。其运行环境主要由大数据分析平台组件构成。

本项目涉网犯罪侦查打击服务平台研发涉及网络空间测绘技术、大数据挖掘技术、侦查过程再造等，相关技术主要研发内容及在产品中的应用如下：

技术方向	主要研发内容	相关技术在产品中的应用
网络空间测绘技术	用搜索引擎技术提供交互，让基层公安机关可以方便的搜索到网络空间上与涉网犯罪相关的情报。用各种测绘方法描述和标注网络位置，用主动或被动探测的方法，来跟踪网络空间上情报对象的状态和关系，对其进行画像。	作为涉网犯罪侦查打击的基础数据，是案件线索的主要来源，为案件侦查提供研判支撑，也是感知犯罪产业现状的基础。
大数据挖掘技术	基于网络层的特征、区域的特征、时间的特征、DNS 应答的特征、TTL 的特征、域名信息等，使用层次聚类、决策树和 ELM、SVM 和隐含马尔可夫模型、朴素贝叶斯、LSTM 决策树、X-Means"等各类算法，挖掘精准线索，提供预警支撑。	作为涉网犯罪侦查打击服务平台的核心能力，为嫌疑人画像、精准线索发现、案件研判、业态感知提供能力支撑。
侦查过程再造	实现协同研判、沙盘推演、辅助研判等联合作战功能，提供数据提取、APK 逆向分析等关键项的靶向分析	实现多警种协同作战，将不同警种的能力和数据以案件目标为载体进行聚焦，实现复杂目标的联合打击

3、项目必要性

（1）传统犯罪加速向以互联网为媒介的非接触式犯罪转移，专业涉网犯罪侦查打击支撑工具及技术的需求迫切

我国信息社会的快速发展、互联网的快速普及使犯罪结构发生了深刻变化，传统接触式犯罪加速向以互联网为媒介的非接触式犯罪转移，传统犯罪的组织方式、外在表现形式发生了持续动态的变化。目前，我国涉网犯罪呈现出案件持续高发多发、网络诈骗迅猛增长、诈骗窝点快速转移、作案群体逐步泛化、黑灰产业日益泛滥等特点，网络违法犯罪情况错综复杂，侦破难度大大提升。

涉网犯罪的日益严峻催生了公安机关采购新型涉网犯罪侦查打击服务的需求。涉网犯罪侦查打击服务平台基于浦东公安实际业务场景，利用大数据技术，开展犯罪行为监测预警、犯罪线索智能落地、辅助案件研判、犯罪业态感知、本地产业评价等业务，能够促进涉网犯罪打击能力的迅速提升，有利于提高我国网络安全综合治理能力和水平，推进构建安全清朗、和谐稳定的网络空间。

（2）本项目是公司顺应客户采购模式变更的重要举措

经过多年的公安信息化建设，我国各级政府及公安部门购买了大量安全软硬硬件产品进行本地化部署。在科技快速发展的时代背景下，安全产品迭代更新加快，公安部门存在安全建设投入较大、安全产品重复购买等问题，也对公安网警

业务培训提出了更高要求。考虑到该等安全产品本地化部署问题，公安机关采购需求呈现向服务化转变趋势。SaaS 服务采用后台自动升级的方式进行技术迭代，避免了重复购买的问题，同时，SaaS 平台受众多，软件升级成本由全国范围内所有需求者共同承担，可以大幅度减轻地方财政负担。云计算产业的快速发展带动虚拟化及云服务理念的持续渗透，也进一步吸引公安机关放弃传统的软硬件产品购置，进行服务采购。未来公安客户将倾向于集中采购安全运营服务，实现一网统办、一网统管，主动、强力、持续的综合性涉网犯罪侦查打击技术服务将成为新需求。

公安部门是公司最主要客户群体之一，2017-2019 年度，来自公安部门的收入占公司主营业务收入的比重均超过 10%。本项目拟采用云计算方式实现技术服务交付模式的转型，相比产品销售或定制化研发项目模式，服务模式更符合客户采购方式的变化，能够提升公司市场竞争力。同时，本项目有利于推动涉网犯罪侦查打击技术的更新迭代，为基层警力提供技术赋能，将办案模式由传统的被动式侦破升级为主动打击，进一步绑定公安客户、提升客户粘性。

（3）本项目为公司未来市场拓展提供重要基础

本项目拟落地的上海浦东新区具备良好的网安工作基础，且作为沿江经济发达地区，拥有以金融为代表的投资服务行业，以贸易平台、网上零售、新型购物中心等为代表的新经济行业和以“中国芯、创新药、蓝天梦、未来车、智能造、数据港”为代表的六大核心产业。该等产业相关企业的发展依赖于大数据、人工智能和互联网信息共享流通，对网络犯罪而言是具有高价值的重点攻击对象，也是涉网犯罪的高风险企业。浦东新区公安干警案件侦查的丰富经验和高风险企业集聚环境为公司涉网犯罪侦查打击服务平台的研发和建设提供了业务经验和高频样本，有助于平台专题库的建设和完善。本项目立足浦东公安良好的网安工作基础和区域典型高频样本，有效保障了公司涉网犯罪侦查平台对复杂涉网犯罪案件的侦查能力，对后续全国各地平台的建设推广具有较强的可借鉴性。此外，本项目通过涉网犯罪侦查打击服务的拓展，有利于加强与公安部门的业务协作，在拓展涉网犯罪安全服务需求的同时，有助于进一步带动公司网络安全产品在公安领域的应用与推广，为公司未来市场拓展提供重要基础。

4、项目可行性

（1）国家加强对公安机关打击涉网犯罪的政策支持力度，为本项目拓展提供政策保障

伴随信息社会不断发展，人民生产生活加速向网上转移，利用通讯工具、互联网等技术手段实施的电信网络诈骗犯罪活动时有发生，严重侵害人民群众财产安全和其他合法权益，社会危害巨大。为有效控制涉网犯罪案件的发生，加强涉网案件的打击侦查能力，国家正不断加大政策支持力度。

2016 年 12 月，最高人民法院、最高人民检察院和公安部联合印发《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》，强调要依法严惩电信网络诈骗犯罪，全面惩处关联犯罪，坚决有效遏制电信网络诈骗等犯罪活动，努力实现法律效果和社会效果的高度统一；2018 年 6 月，公安部印发《网络安全等级保护条例（征求意见稿）》，明确网络运营商在打击违法犯罪活动、保障网络信息安全方面的义务，指出公安机关应根据有关规定处置网络安全事件，依法查处危害网络安全的违法犯罪活动；2018 年 9 月，公安部印发《公安机关互联网安全监督检查规定》，规范了公安机关互联网安全监督检查工作，为预防网络违法犯罪，维护网络安全制定了法律依据。此外，近几年，最高人民法院、最高人民检察院多次发布关于具体领域涉网犯罪案件适用法律若干问题的司法解释。该等政策法规的相继出台明确表达了我国始终保持对涉网犯罪严打高压态势的决心，为本项目提供政策可行性。

（2）我国涉网犯罪侦查打击规模大，为项目实施提供了良好市场空间

截至 2020 年 3 月，我国网民规模已达 9.04 亿[3]，随着信息通讯技术的普及，涉网犯罪日益猖獗，发案数量激增，涉案金额巨大，社会影响恶劣。公安部门组织进行了多次打击涉网犯罪专项行动。2018 年，全国公安机关开展“净网 2018”专项行动，侦破各类网络犯罪案件 5.7 万余起[4]；2019 年 1-10 月，开展“净网 2019”

[3]数据来源：《第 45 次中国互联网发展状况统计报告》

[4]数据来源：中国新闻网《“净网 2018”专项行动侦破网络犯罪案件 5.7 万余起》

专项行动，侦破涉网案件 4.6 万余起[5]；2020 年，公安部组织开展“云剑-2020”、“长城 2 号”、“510”等专项打击行动。2020 年上半年，全国共破获电信网络诈骗案件 10.1 万起。

本项目主要为公安部门提供涉网犯罪侦查打击技术与平台服务支持，面对我国涉网犯罪高发多发的严峻态势以及各级公安机关从严从重从快打击涉网犯罪案件的态度，相关部门对涉网犯罪侦查打击的专业辅助技术工具及服务需求快速提升，为本项目提供了良好的市场保障。

（3）本项目具备良好的技术、人才和客户基础

本项目主要客户为公安部门，经过多年的业务发展，公司在公安领域积累了深厚的客户基础。在涉网犯罪领域，公司曾多次收到浦东网警和经侦部门提出的协助进行涉网犯罪侦查需求，为公安机关提供了关键性辅助工作，获得了较高的客户认可度。在与公安部门多年的合作中，公司在涉网犯罪侦查打击领域已经形成一定的技术和人才积累。本项目产品属于行业内较前沿产品，主要涉及大数据关联分析、嫌疑人目标画像技术和案件线索主动发现技术等，公司在相关领域已积累了部分技术与专利，具备良好的技术基础，未来将进一步加强技术原型研发。同时，公司在业务开展过程中，除网络安全研发人才外，积累培育了一支协助公安部门调查涉网犯罪的技术服务团队，以及需求分析和功能设计相关的人才队伍，为本项目的顺利实施提供了必要的人才储备。

公司良好的产品技术和人才积累，以及与下游公安客户紧密的合作关系为本项目的顺利实施提供了可靠保障。

5、投资概算

本项目预计建设期为 3 年，项目总投资 13,006.66 万元，拟投入募集资金 10,216.18 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额

[5]数据来源：公安部《“净网 2019”专项行动共侦破涉网案件 4 万余起抓获犯罪嫌疑人 6 万余名》

1	**工程建设费用**	**5,806.22**	**4,291.10**
1.1	场地租赁费	1,515.12	-
1.2	场地装修费	864.00	864.00
1.3	硬件购置	2,434.60	2,434.60
1.4	软件购置	992.50	992.50
2	**研发费用**	**5,925.08**	**5,925.08**
3	**基本预备费 2%**	**234.62**	-
4	**铺底流动资金**	**1,040.74**	-
	合计	**13,006.66**	**10,216.18**

6、实施主体、项目选址和建设期限

本项目实施主体为公司全资子公司上海安恒智慧城市安全技术有限公司。项目拟在上海浦东新区租赁办公场地，研发落地涉网犯罪侦查打击服务平台，预计建设期为 3 年。

2020 年 9 月，公司子公司上海安恒智慧城市安全技术有限公司已就项目所需用楼与上海张江高科技园区开发股份有限公司签署《房屋租赁合同》。

7、项目备案和环评情况

截至本预案出具日，本项目的可行性研究报告已编制完毕，公司正在办理备案等相关事项。

8、项目经济效益评价

经测算，本项目税后内部收益率为 23.27%，税后静态投资回收期为 6.64 年，项目预期效益良好。

（三）信创产品研发及产业化项目

1、项目概况

信息技术应用创新产业是国家构建安全可控的自有 IT 产业的重要基础，已经成为经济数字化转型、提升产业链发展的关键。为了解决本质安全问题，大力发展信创产业已上升为一项国家战略。2016 年 4 月 19 日，网信工作座谈会明确提出，“核心技术受制于人是我们最大的隐患”，同年，国家再次强调“抓紧突破网络发展的前沿技术和具有国际竞争力的关键核心技术”。在中美关系动荡之际，信创产业受到了各界的广泛关注，建设安全可控的信息技术体系成为“新基

建”和“数字中国”战略的重要内容。国产化的 IT 底层架构不断完善使得国产化替代加速推进，我国信创产业进入快速发展时期。

信创产业主要包括新一代信息技术下的云计算、软件（操作系统、中间件、数据库、各类应用软件）、硬件（芯片、GPU/CPU、主机、各类终端）、安全（网络安全）等领域，涵盖了 IT 底层基础软硬件到上层应用软件的全产业链。随着云计算、大数据、物联网等新技术的发展应用，网络安全应用场景更加复杂，网络攻击组织性与目的性不断加强，社会危害性不断加大。网络安全建设作为信创产业的重要组成部分，自主创新需求更加迫切。

本项目拟在杭州滨江区安恒大厦临近地块自建办公用楼，开展信创产品线开发、适配和产业化基地建设，同时建立省级信创适配实验室，逐步完成国产化技术路线适配工作，搭建符合国家网络安全法、国家密码管理法等法规要求的完善的信创产品体系，为客户提供定制化信创产品和基于国产化环境的网络安全解决方案。此外，项目还将加强网络资产测绘、新型未知威胁发现、攻击溯源等关键技术的研发，以适应日益复杂的网络安全环境，强化公司信创业务集成能力，在抓住信创产业发展机遇的同时，进一步提升公司的综合竞争优势。

2、项目建设内容

信创产品的研发重点在于国产化适配工作，目前公司现有网络安全基础产品和平台产品的国产化适配工作已按计划开展。除此之外，为了更好地满足客户技术方案的要求，本项目拟加强攻击识别、行为分析、流量分析、追踪溯源等关键技术研发，相关技术主要研发内容及在产品中的应用如下：

技术方向	主要研发内容	相关技术在产品中的应用
攻击识别	攻击行为识别技术研究	对攻击产生的影响进行判定，形成完整的入侵分析，对各种来源的攻击行为进行确认和归类确保原始攻击行为有效性，进一步挖掘和攻击链分析，降低攻击分析难度、提升效率，快速发现异常入侵，提升安全响应能力。
行为分析	自动化行为分析与自验证技术研究	对各种来源的攻击行为进行确认和归类确保原始攻击行为有效性，进一步挖掘和攻击链分析，降低攻击分析难度、提升效率，快速发现异常入侵，提升安全响应能力。
流量分析	对实时网络流量分析的深度检测技术研究	借助网络流量分析和持续监控，使用沙箱技术、实时监测方法与系统等，监测提取异常行为。
追踪溯源	追踪溯源、攻击画像的分析技术研究	通过行为识别和监测提取，进行安全专家分析和大数据分析，提供高价值的威胁情报信息及追踪

		溯源的线索，具有重要的现实意义。
实体画像与特征自动更新技术	对实体画像进行数据建模，结合业务实际的需求，找出相关的数据实体，以数据实体为中心规约数据维度类型和关联关系，形成符合业务实际情况的建模体系。	应用于用户实体行为特征提取与分析模块，实现对实体行为特征的提取。
复杂网络的资产自动重识别技术	提出双栈协议识别技术实现不同网络环境的发送协议识别；提出地址归一化技术，实现将识别到的不同类型的地址解析归一化为相同的地址格式；通过构建外部资产地址库，以实现对不同资产的识别和归类	应用于资产发现与管理模块，实现对复杂网络环境下，不同的日志传输方式、不同的传输协议以及不同的网络之间的资产识别。
面向对象的安全数据分层技术	采用“分层解耦”的设计理念，根据数据的流转方式，进行数据分层设计，各层之间采用集中的数据总线进行数据传输和交换，以此降低各类安全应用对底层数据存储之间的强依赖性	应用于安全大数据中心，实现数据的分层分类存储，为业务功能模块提供数据支撑。
基于语义化安全日志聚类的异常行为检测技术	设计基于语义化分析的安全日志聚类模型，采用向量相似度计算算法，计算日志元素间的相似度，得到历史日志间的相似度之后，采用聚类算法对其进行分组计算，快速将日志分类	应用于异常行为分析模型的建立，通过对系统异常行为的监测，可以发现未知的攻击模式。异常行为检测的关键在于建立正常使用模式并利用该模式对当前用户行为进行比较和判断。
基于知识图谱的网络攻击自动化关联推理技术	从资产、威胁和脆弱性三个方面进行网络空安全威胁建模技术研究，主要研究网络空间中安全威胁的行为特征、生成机理、攻击流程、危害效果等建模技术	应用于威胁感知模块，实现从资产、拓扑、网络空间多方面的风险检测与感知。
安全管理	安全服务实例的管理与编排	在云安全管理平台上统一管理编排安全组件，实现安全组件的生命周期管理，兼容纳管第三方安全组件。
资产中心	资产管理与风险评估	实现对租户资产信息同步统一管理，一键下发安全检查任务，协助用户发现资产漏洞与安全威胁。
网络安全	安全能力评估与运营	借助运营平台分析评估租户整体安全状态，协助管理员评估租户安全态势，分析租户安全缺陷。
操作系统安全	针对国产操作系统进行深度研究	1、进行操作系统安全代码研究、内核安全测试、Oday 漏洞跟踪、SRC 应急响应中心建设； 2、操作系统安全状态研究、桌面、服务器病毒、木马攻击防护、主机 IDS 防御性研究； 3、APP 市场安全研究、APP 漏洞研究、沙箱安全研究、SDK 安全研究； 4、全生命周期安全响应流程适配研究、客户现场应急响应工作研究、安全取证、恢复研究；

		5、安全管理流程闭环研究。
数据库、中间件、应用安全研究	针对国产数据库、中间件、各类应用进行安全研究	1、安全机制研究，开展程序自身安全保护机制、沙箱环境等研究； 2、0DAY 研究，积极展开安全厂商、应用软件之间的漏洞研究、修复、通告等机制； 3、安全生态研究，依托操作系统 SRC，形成操作系统、应用软件、安全厂商、监管机构安全生态闭环。
CPU 安全	针对各类国产 CPU 漏洞、加密技术的研究	1、研究各类技术路线 CPU 可能具有的架构漏洞； 2、研究 CPU 集成硬件级安全芯片，与 CPU 厂商一同研究、开发安全芯片的操作系统级应用，研究安全整合方案。

3、项目必要性

（1）本项目顺应我国信息安全产品国产化替代的必然要求

信息技术应用创新产业是国家构建安全可信的自有 IT 产业的重要基础，是国家经济数字化转型、提升产业链发展的关键。从“华为、中兴事件”体现出我国科技产业受制于人的现状制约了经济发展。2020 年 5 月 15 日，美国商务部在全球范围内限制使用美国软件和技术的公司向华为提供半导体等产品，中国芯片、系统的断供威胁持续增大，信息技术产业创新的必要性和紧迫性愈发凸显。为解决本质安全问题，信创作为国家战略成为我国“新基建”的重要内容。同时“数字中国”战略提出了建设“2+8”安全可控体系，标志着 2020-2022 年成为国家安全可控体系推广的重要时期。国家对信息安全愈加重视，各级政府积极建立基于国产化的 IT 底层架构和标准，信创产业发展势头强劲，国产化替代形势不可逆转。

本项目依托公司在网络安全领域的产品技术和人才基础，依据国家战略要求，对基础网络安全产品、云安全平台、态势感知平台和安全运营平台等进行国产化适配。同时项目将基于国产化平台，全面开展信创领域的安全咨询、安全集成、安全运营等工作，加强对运维访问控制审计技术、分布式漏洞发现与验证技术、基于云架构的安全扫描与监测技术、SaaS 化云安全防护等技术的研发力度，有助于提升公司新一代网络安全产品研发能力，推进和适应我国信息产品国产化替代趋势。

（2）国产化 CPU 及操作系统已基本完成国产化替代，下游国产化软硬件需求逐步显现

目前，国产 CPU、操作系统已经实现从“能用”到“好用”的跨越，以龙芯、飞腾、兆芯、申威、海光、鲲鹏为代表的国产 CPU，以及以中标麒麟、银河麒麟、统信 UOS 为代表的国产操作系统，已经初步具备替代能力。

随着国产 CPU、操作系统等基础设备完成国产化替代布局，下游软硬件产品的国产化替代进程趋势明朗。过去国内一定程度上存在“重硬轻软”的情况，软件与智能硬件相比较少受到关注，随着“中国制造 2025”计划出台，近年来国家政策和地方政策逐渐向软件倾斜，为我国自主研发的软件发展注入了强心剂。2020 年 8 月 4 日，国务院印发《新时期促进集成电路产业和软件产业高质量发展的若干政策》，此次政策将软件产业核心技术的研发提升举国体制的新高度，强调以国家科技重大专项的方式支持软件产业，引导资金、人才向软件产业转移。

由于自主可控的产业链条上各生产环节的企业存在紧密的分工协作关系，上游的 CPU、操作系统等基础产品的更新换代促使下游软件国产化需求空间进一步扩大。公司主要客户政府、公安、电信运营商、金融企业等机构对于安全性、可控性要求的不断提高，在国产软件技术达到替代标准的情况下，开始引入软件技术自主可控的集采要求。本次信创产品研发及产业化项目是公司顺应国产替代安全可控大趋势，满足软件技术可控集采要求的必然选择，是公司保持并提升主要下游市场竞争力的重要战略。

（3）信创产业发展势在必行，公司急需顺应趋势完成信创产品及市场布局

随着国产 CPU、操作系统等基础层产品不断完善，信创产业逐步成为当前形势下国家经济发展的新动能，以 2020 年为起点，信创产业开始全面推广，预计 2020 年我国自主可控的计算机市场规模约为 1.05 万亿，到 2025 年市场规模将达到 1.3 万亿；未来 3 年信创领域国产芯片替代空间达 220 亿元；操作系统领域由于外资厂商高度垄断，未来 3 年信创领域国产操作系统替代空间可达 264 亿元，我国信创产业发展空间巨大。伴随安全自主可控的信息化建设进程的推进，下游客户对信创网络安全产品和服务需求强烈，行业市场空间广阔。

在信创产业的不断发展下，国产化替代将从电信运营商、政府、金融等关键敏感行业逐步向全行业展开。中国移动在 2020 年 7 月大规模采购国产数据库用于 OLTP 自主可控数据库联合创新项目，明确要求各参与投标的厂商拥有自主知

识产权、产品核心代码为投标公司自主研发且具有数据库方面的发明专利，最终国内南大通用、人大金仓、阿里云、万里开源、中兴通讯五家公司中标。根据中国电信公布的 2020 年服务器采集清单，本年度将采购鲲鹏 920 系列处理器或 Hygon Dhyana 系列处理器，年度采购服务器中国产化比例达到了 20%。以银行为代表的金融行业也开始加快国产化替代的脚步，2020 年农行重点采购了 2000 台基于鲲鹏处理器的 TaiShan 服务器，将用于金融行业首个“基于 ARM 架构多路服务器+全开源中间层软件+自研应用”的业务系统。

作为公司重要下游行业，2017-2019 年该等电信运营商、政府、金融等关键敏感行业客户对公司的营业收入贡献比重分别达到 50.93%、51.94%和 48.71%。公司需要持续满足这三类客户对安全产品及服务的需求，建立与客户的良好合作关系，保持公司长期收入的稳定。面对该等客户已逐步实施的国产化替代采购策略，提前进行信创领域布局是公司维系客户巩固市场份额的重要举措。

信创行业暂未出现垄断性国产化平台，目前市场同时存在龙芯、飞腾、兆芯、申威、海光、华为海思等主流国产 CPU 以及中标麒麟、银河麒麟、中科方德、神威睿思、深度、普华等主流国产操作系统，不同客户基于业务需求，会自主选择不同品牌的 CPU 和操作系统，各 CPU 与操作系统适配技术差异较大，需网络安全厂商进行针对性的适配、改造与研发，一定程度上丰富了细分市场，推升了信创产业的市场空间。

包括北信源、蓝盾股份在内的多家同行业信息安全厂商陆续通过各类直接或间接融资方式投资布局信创产业化项目。面对未来错综复杂的全球政治格局，国产化替代势在必行，尽早布局信创产业是整体信息安全产业及公司巩固原有市场份额、开拓新增市场的必然战略选择。

4、项目可行性

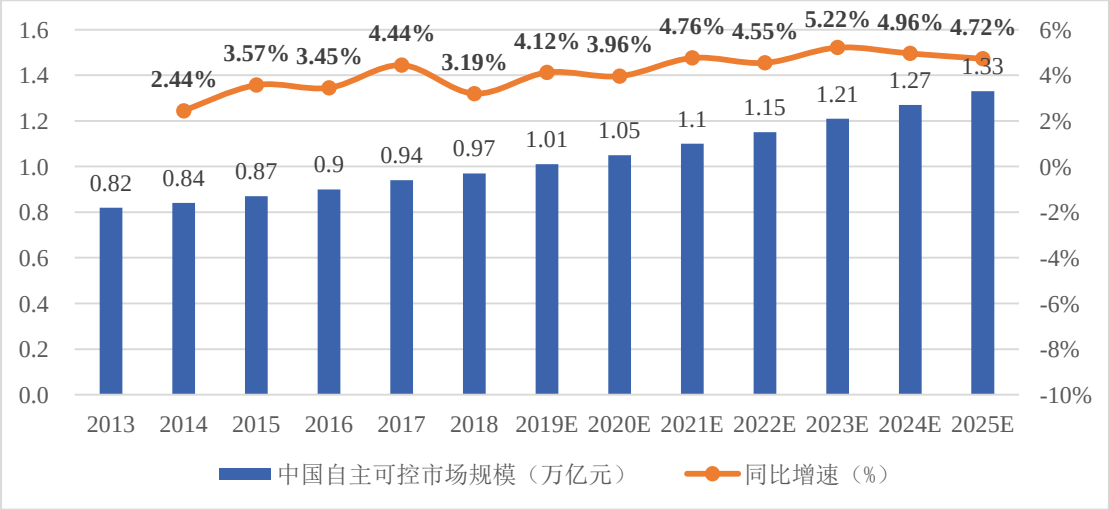
（1）国家高度重视信创产业发展，政策法规日趋完善

近年来，国家高度重视信创产业发展，鼓励信息技术创新驱动国家网络安全行业加快发展。2014 年，科技部、工信部等部门发布了《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》，提出至 2019 年各银行业金融机构对安全可控信息技术的应用达到不低于 75％的总体占比目标。2016

年，中共中央办公厅、国务院办公厅印发了《国家信息化发展战略纲要》指出，到 2025 年根本改变核心关键技术受制于人的局面，形成安全可控的信息技术产业体系。2020 年 4 月 27 日，国家互联网信息办公室、发展改革委、工信部等 12 个部门联合发布《网络安全审查办法》，明确提出采购进口网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险，国外产品进入国内信息基础设施难度加大，国产替代加速。政策的不断完善也使得信创和网络空间国家安全领域有法可依，为行业发展提供了普适性的法律标准与依据，并推动国产化替代产品需求涌现。

（2）我国信创产业市场空间广阔

伴随我国信创产业全面推广，国家预备从基础硬件-基础软件-应用软件三个层级实现对国外产品的替代，信创行业迎来快速发展期。预计 2020 年我国自主可控的计算机市场规模约为 1.05 万亿，到 2025 年市场规模将达到 1.3 万亿；按党政和国企单位 4400 万人测算，未来 3 年信创领域国产芯片替代空间达 220 亿元；操作系统领域内容外资厂商高度垄断，未来 3 年信创领域国产操作系统替代空间达 264 亿元[6]，伴随安全自主可控的信息化建设进程的推进，下游客户对信创网络安全产品和服务需求强烈，行业市场空间广阔。我国自主可控市场规模及增速预测如下图所示：



[6]数据来源：华西证券《信创，重塑中国 IT 产业基础的中坚力量》

数据来源：观研天下

信创产业整体市场空间广阔，并且可供挖掘的细分领域众多，目前可供选择的主流国产化平台包括龙芯、飞腾、鲲鹏、海光、申威、兆芯，每个国产化平台在不同的地区与行业中占据着主流地位，如飞腾在湖南、天津等地落地进度较快，龙芯在军事、航洋钻井平台等行业有着大范围应用。目前，六大主流国产化平台均有各自细分市场，信创行业暂未出现垄断性国产化平台，且不同平台的适配技术差异较大，进一步推升了信创产业的市场空间。

（3）公司丰富的技术积累为本项目实施提供保障

本项目主要建设目的为公司原有安全产品体系的国产化适配研发及产业化，公司原有的网络安全底层技术优势在国产系统适配后仍将保持。公司拥有 48 项网络安全核心技术，并在云安全、大数据安全、物联网安全和智慧城市安全等多个细分市场形成核心技术优势，处于行业领先位置，能够有效保障本次项目公司原有安全产品体系的国产化适配研发及产业化进度。截至本预案出具日，公司已与龙芯、兆芯、鲲鹏、飞腾、申威、海光、统信 UOS、麒麟软件等芯片及操作系统厂商完成了共计 59 份产品兼容性互认证明。公司态势感知平台、天池云安全平台及 AILPHA 大数据平台等平台类产品已全面开展国产化芯片及操作系统适配工作；远程安全评估系统、Web 应用防火墙及综合日志审计等部分网络安全基础产品已完成国产适配转化。

此外，公司在国家信创领域发展中担任了重要角色，帮助公司掌握国家信创发展战略及技术发展方向，进行精准产品研发。公司是信息技术应用创新工作委员会成员单位，参与整机工作组、龙芯工作组、飞腾工作组、鲲鹏工作组、人工智能工作组等的相关工作，同时参加了安全中心技术委员会安全开发治理、安全性测试、关键产品挑战赛、漏洞管理、终端安全 5 个专项组，是安全开发治理专项组的组长。

（4）公司具备开展业务的客户基础

通过持续的市场拓展，目前公司产品及服务已经进入了包括运营商、政府、能源、金融、教育等在内的众多行业，积累了上述领域大量优质客户，并长期保持着深入稳定的合作关系，该等客户所处领域的网络安全关乎国计民生和国家安

全，是国家政策要求的处于优先实现自主可控的核心关键行业，是信创产品的刚需群体，有效降低了本次信创项目市场拓展经营风险和财务风险。

5、投资概算

本项目预计建设期为 3 年，项目总投资 62,122.22 万元，拟投入募集资金 45,870.82 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**32,522.61**	**31,166.61**
1.1	土地款	1,356.00	-
1.2	场地建造费	24,892.61	24,892.61
1.3	硬件购置	3,314.00	3,314.00
1.4	软件购置	2,960.00	2,960.00
2	**研发费用**	**23,555.21**	**14,704.21**
3	**基本预备费 2%**	**1,121.56**	-
4	**铺底流动资金**	**4,922.84**	-
	合计	**62,122.22**	**45,870.82**

6、实施主体、项目选址和建设期限

本项目实施主体为安恒信息。项目拟在杭州滨江区安恒大厦临近地块自建办公用楼，进行信创产品线开发、适配和产业化基地建设，预计建设期为 3 年。2020 年 7 月，公司已就本项目建设所需用地与杭州市规划和自然资源局签署《国有建设用地使用权出让合同》。

7、项目备案和环评情况

截至本预案出具日，本项目的可行性研究报告已编制完毕，公司正在办理备案等相关事项。

8、项目经济效益评价

经测算，本项目税后内部收益率为 25.07%，税后静态投资回收期为 6.55 年，项目预期效益良好。

（四）网络安全云靶场及教育产业化项目

1、项目概况

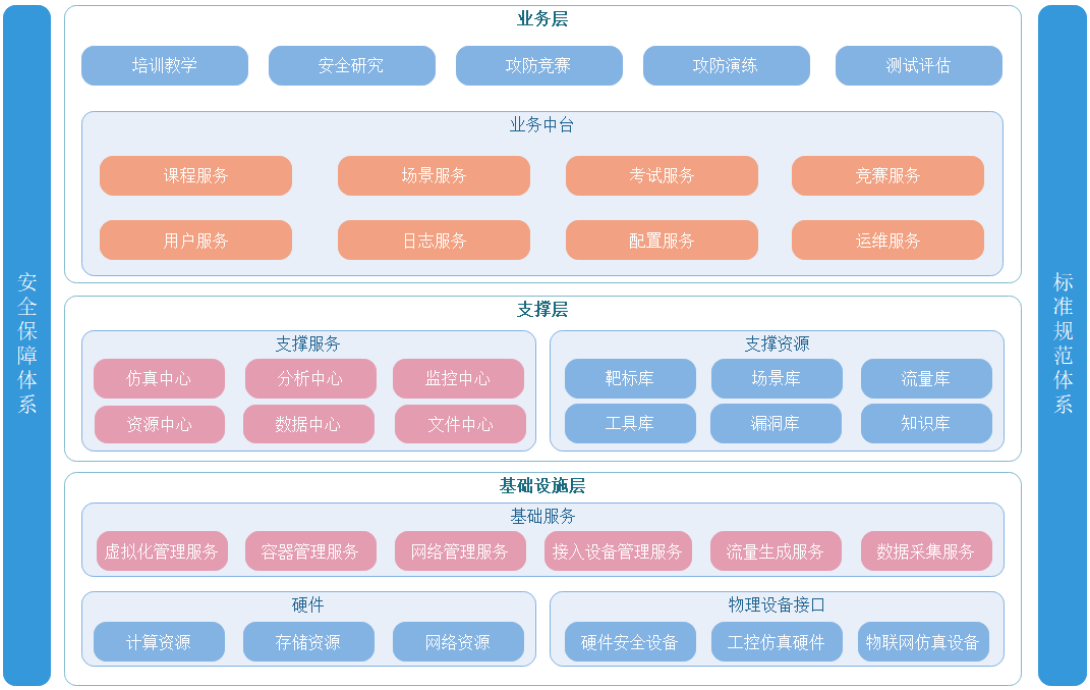
近几年，随着《网络安全法》的出台，各级政府和企业在网络安全建设方面的投入不断加大。我国网络安全人才需求迅速攀升，根据新华网报道，截至 2019 年 9 月，我国网络空间安全人才数量缺口高达 70 万，预计到 2020 年将超过 140 万。2016 年 12 月，国家互联网信息办公室印发《国家网络空间安全战略》，提出实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境；2020 年 7 月，全国人大常委会印发《数据安全法（草案）》，再次指出要采取多种方式培养数据开发利用技术和数据安全专业人才。各地政府鼓励网络安全相关学科建设，启动区域网络安全实训基地建设，加强网络安全人才培养成为增强国家网络安全实力的重点，网络安全教育市场空间广阔。

公司作为专业的网络信息安全服务提供商，拟结合现有产品和技术优势，加强公司在教育领域的业务拓展。本项目拟在杭州市滨江区新建办公楼的部分楼层进行包括网络安全靶场在内的网络安全演训产品及网络安全靶场云化部署的研发及产业化。项目将建设网络安全靶场平台，为参与培训的学员提供网络空间仿真实训竞技平台，以“学、练、测、评”一体化设计的方式加强学员专业技能。同时将网络安全靶场和安全综合实验室进行云化部署，建立 SaaS 化网络安全云靶场平台，结合网络安全教学产品和认证服务实现平台、教学内容和服务一体化，开展以实战能力养成为导向的网络安全培训服务。此外，本项目还将对公司目前商用网络安全基础及平台产品进行教育培训适用化开发，为学校、大型企业和政府提供专业信息安全培训工具。

本次项目的建设实施有助于扩展公司网络安全教学类产品市场空间，开展以实战为导向的网络安全培训服务，对网络安全人才培养产品和服务进行一体化升级，从横向上扩展公司业务线。另一方面，公司为学校、大型企业和政府建设网络安全靶场提供相应的产品，有助于加强潜在用户对公司产品的认知，推广相关网络安全产品，推进公司产品生态建设。项目有助于满足国家培育行业人才战略的需要，拓展新的产品业务领域，进一步提升行业整体竞争力，推动公司业绩增长。

2、项目建设内容

靶场平台采用分层化服务的设计理念，将系统的整体架构分为三个层次和两个体系。三个层次分别为基础设施层、支撑层和业务层，两大体系为靶场平台的安全保障体系与靶场本身的标准规范体系。系统架构示意图及各部分主要功能如下：



①基础设施层：作为整体靶场平台的底座，主要包含了靶场需要的基础硬件资源及基础服务两大部分。其中，基础硬件主要包括资源硬件及物理仿真设备接入；基础服务是底层硬件与靶场上层应用的连接通道，通过基础服务的封装将基础硬件能力开放给靶场上层应用使用，具体包括虚拟化管理服务、容器管理服务、网络管理服务、接入设备管理服务、模拟仿真服务和数据采集服务。

②支撑层：是靶场平台的核心能力，在基础服务的基础上结合靶场的业务需求进一步封装，给上层业务提供更加标准化的能力封装，主要包括支撑靶场正常运行的支撑资源库和支撑靶场上层业务的核心支撑服务两部分。其中，支撑资源包括靶标库、场景库、仿真库、工具库、漏洞库和知识库；支撑服务包括资源中心、数据中心、仿真中心、分析中心和监控中心。

③业务层：是靶场的核心业务体现，根据整体架构的设计原则，采用微服务架构，开发通用的业务能力中台，主要内容包括用户服务、配置服务、运维服务、

日志服务、课程服务、考试服务、竞赛服务和场景服务，并在中台基础上包装了培训学习、安全研究、攻防竞赛、攻防演练、测试评估等主要的靶场业务形态。

本项目网络安全靶场产品研发涉及虚拟网络构建技术、多维网络互联技术、镜像资源管理技术、大规模虚拟节点快速部署技术、背景流量模拟技术、用户行为模拟技术、并行任务安全隔离技术、复杂网络下全量数据采集技术等，相关技术主要研发内容及在产品中的应用如下：

技术方向	主要研发内容	相关技术在产品中的应用
虚拟网络构建技术	软件定义网络、链路仿真、网络节点生成等技术研究	在靶场平台的目标网络环境构建中，实现虚拟网络的构建
多维网络互联技术	虚实互联、多网互联接入等技术研究	在靶场平台中目标网络环境高逼真还原及大规模网络仿真中，实现非虚拟化网络的快速接入及多仿真场景快速互联，形成规模化网络
镜像资源管理技术	大规模镜像存储、跨网镜像高速传输等技术研究	在靶场平台的底层资源管理中，实现镜像资源多服务间快速的同步
大规模虚拟节点快速部署技术	虚拟节点、容器节点、离散事件节点在大规模构建情况下实现快速部署的技术研究	在靶场平台的目标网络靶标构建中，实现靶标资源的快速构建
背景流量模拟技术	真实流量录制、流量拼接、流量叠加、混合流量生成与回放等技术研究	在靶场平台的目标网络构建环境仿真中，实现场景真实流量状态还原
服务、应用、用户行为模拟技术	服务行为复制、用户行为复制、软件模拟、模型模拟、协议模拟及多行为协同模拟等技术研究	在靶场平台的目标网络构建环境仿真中，实现场景真实服务、应用及用户行为复现
并行任务安全隔离技术	并行任务网络隔离、数据隔离、软件隔离等技术研究	在靶场平台的实际使用过程中，当多个任务在靶场中进行的时候，要实现多个任务所对应的目标网络环境的隔离、多个任务各自采集的相关数据隔离以及整个过程中涉及到的软件等相关资源隔离
复杂网络下全量数据采集技术	虚拟网络中流量采集、终端数据采集、全节点日志采集、可编辑数据采集、可插拔终端数据采集器等技术研究	在靶场平台的实际工作过程中，实现对靶场目标网络环境中的相关数据进行全量的采集
攻防数据分析技术	安全事件分析、用户行为分析、KillChain 分析、追踪溯源、安全态势等技术研究	在靶场平台的运行过程中和完成相关任务后，实现对靶场目标网络环境整体安全态势、整体任务过程、任务结果进行综合分析
半自动化攻击技术	半自动化攻击链构建技术研究	在进行攻防训练和演练的时候可以通过实现对目标环境的攻击及测试
安全评估技术	人员安全能力评估模型、设备安全评估模型设计与研究	在靶场平台的测试评估过程中对训练人员、被测试的设备和环境进行安全评估
异构虚拟化平台统一接入技术	异构虚拟化平台统一接入技术实现	在靶场平台的节点生成中，实现对异构虚拟化平台快速适配

3、项目必要性

（1）项目建设为我国网络安全人才培养提供了有效工具

随着我国信息化进程不断深入和《数据安全法》等政策法规的出台，保障数据安全的重要性越发凸显，企业对网络安全人才培养领域的投入持续加大。网络安全团队需要以业务为导向，积极构建业务与网络安全之间的共生关系。同时，伴随等保 2.0 等新标准的实施，我国网络安全建设已从单一安全走向整体安全，对网络安全人才提出了更高的要求，网络安全人才培养的能力和水平亟待提高。

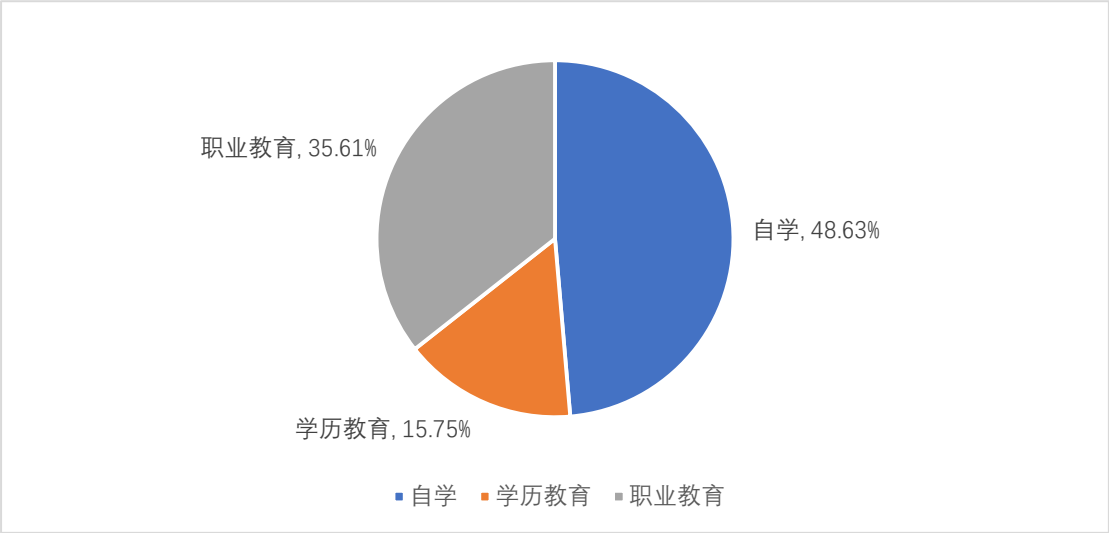
目前，我国网络安全人才培养的主要途径是大学教育，但相关专业发展时间较短，且偏重理论教学，缺乏实践和参与产业实践的机会和动力，知识更新速度较慢，存在学生理解较浅、培养目标不明确、学生自身能力和实战化能力的培养较为缺乏等问题。

本项目基于网络安全行业人才紧缺的现状，以及当前学历教育与职业技能水平不匹配的问题，为网络安全人才培养提供了环境、专业工具和业务形态支撑，有助于解决高层次专业教师缺乏，教材良莠不齐，缺乏攻防演练平台，综合性、自主防御性试验难以构建和学生缺少实战等问题。通过网络安全靶场平台产品研发，加强现有网络安全产品向适用于教育教学产品的转化研发，为我国网络安全教学内容建设和网络安全人才培养提供实战化培训工具，有利于丰富我国网络安全人才培养模式，提高网络安全人才培养能力和水平，进而满足日益增长的网络安全人才需求。

（2）本项目是公司加强网络安全教育市场拓展、抢占市场份额的重要举措

伴随网络安全行业的快速发展，网络安全人才出现了较大缺口，根据新华网报道，截至 2019 年 9 月，我国网络空间安全人才数量缺口高达 70 万，预计到 2020 年将超过 140 万。面对市场巨大的人才需求缺口，校企合作、企业内训及职业类培训等人才培养模式加速发展，以人才培养和系统测试为驱动的网络安全教育培训需求快速增长。2019 年，我国网络安全行业“自学型”求职者占比达

48.63%、“职业教育型”求职者占比 35.61%，自学和职业教育已经成为求职者获取网络安全知识和技能的主要方式[7]。



数据来源：360 网络安全大学人才研究院

面对持续增长的市场空间，同行业领先企业相继开始布局网络安全人才教育市场，天融信、奇安信等企业设立专攻校企合作销售团队，天融信、启明星辰以及绿盟科技均设有网络安全培训学院，而蓝盾股份等企业已着手投资建设网络空间仿真靶场实训项目。尽管公司在网络安全教育行业已有所布局，成立了网络空间安全学院，但是尚未具备专属的教育培训自主产品与服务生态，目前采取的主要方式是依附于公司商业化产品提供网络安全教育培训附加服务，针对专业教育培训的适配性较低。本项目将通过加强网络安全靶场产品研发和网络安全人才培训服务改善现状。通过网络安全靶场产品研发，有助于扩展公司教学类产品市场空间，升级以实战为导向的网络安全培训服务，实现网络安全人才培养产品和服务一体化升级，完成专业网络安全教育培训业务布局，从横向上扩展公司业务线。

（3）项目建设利于公司选拔网络安全人才

专业人才稀缺是网络安全行业近年发展的痛点。根据智联招聘发布的《2019 网络安全人才市场状况研究报告》，网络安全人才市场的需求在三年的时间内，扩大到了 2016 年初的 10 倍以上。目前我国每年网络安全学历人才培养数量不足

[7]数据来源：360 网络安全大学《2019 网络安全行业人才发展研究报告》

1.5 万，网络空间安全人才培养的数量远远满足不了社会需求。2019 年，“等保 2.0”的发布及正式执行，对互联网企业、安全厂商、各大政企单位提出更高的安全合规要求。该等制度的落实推动了网络安全人才的需求增长，网络安全人员的需求缺口进一步扩大。人才是网络安全行业各企业的核心资源，专业从业人员的数量、质量、结构和作用的发挥，直接关系到网络安全企业专业水平和服务质量。

近年来随着公司业务规模的快速增长，网络安全人才需求大幅提升，在不断提高招聘力度的情况下，公司校招缺口仍达到 200-300 人。在行业高速发展的背景下，公司未来网络安全人才存在持续性缺口。

网络安全人才培养服务下游用户主要包括在校学生及网络安全从业人员。提供网络安全培训服务有利于公司在网络安全人才稀缺的社会背景下精准发现并锁定相关人才，从而推动公司人才团队的建设与壮大，为长远发展注入优秀新鲜的血液，进一步提升公司在行业内的人才优势。

（4）项目有助于连接与协同下游客户，推广公司网络安全生态

公司为学校、大型企业和政府建设网络安全靶场，提供网络空间安全教育服务与产品，由于相关教育产品均演化自公司原有商业产品，开展教育业务有助于深化潜在用户对公司商业产品体系的认知和应用。此外，网络安全防护产品由于具有适配性与衔接性，不同公司的网络安全产品互不相通难以混合使用，产品学习及转换成本较高，公司将打造基于原有自主研发商用产品的教育专属培训产品体系，教育培训产品的应用能够有效推广宣传公司商业产品体系，从源头更好地绑定潜在客户，促进公司商业产品体系的未来销售。

4、项目可行性

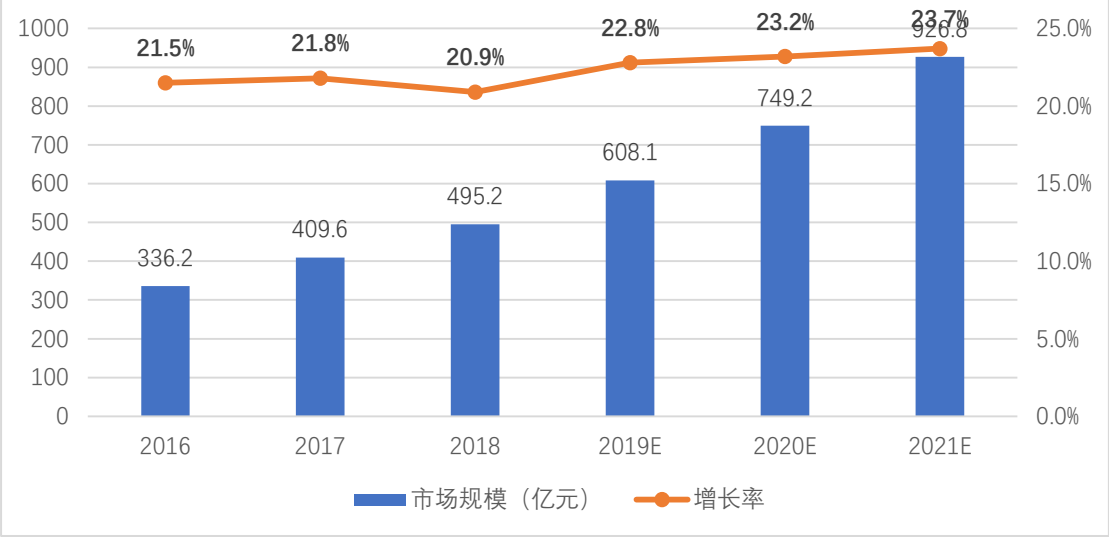
（1）国家对网络安全人才培养的重视为本项目提供了良好的政策保障

伴随全球数字经济蓬勃发展，网络安全的基础保障作用和发展驱动效益日益突出，网络安全人才队伍建设成为保障国家战略安全的重点之一。2016 年 11 月，全国人大常委会颁布《中华人民共和国网络安全法》，明确指出国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，鼓励采取多种方式培养网络安全人才，促进网络安全人才交流；2016 年 12 月，国家互联网

信息办公室印发《国家网络空间安全战略》，提出实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区，形成有利于人才培养和创新创业的生态环境；2017 年 7 月，国家互联网信息办公室印发《关键信息基础设施安全保护条例（征求意见稿）》，强调要培养和选拔网络安全人才，提高关键信息基础设施的安全水平；2017 年 8 月，教育部等多部门联合印发《一流网络安全学院建设示范项目管理办法》，决定于 2017 年至 2027 年实施一流网络安全学院建设示范项目，提升网络安全教育能力；2020 年 7 月，全国人大常委会印发《数据安全法（草案）》，再次指出要采取多种方式培养数据开发利用技术和数据安全专业人才。相继出台的关于促进网络安全人才教育的政策法规，有效保障了本次项目建设及未来实施运营的稳定性。

（2）网络安全市场快速发展，人才教育需求旺盛为本项目提供市场保障

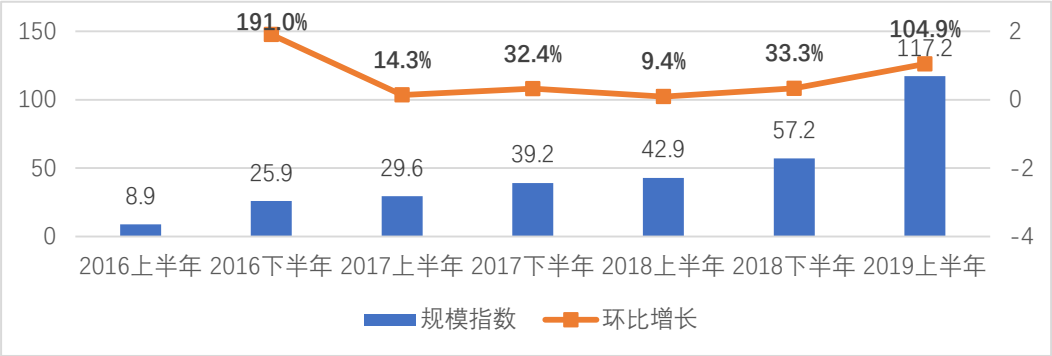
随着我国信息技术的快速发展，网络安全需求激增，带动我国网络安全市场快速发展，预计到 2021 年我国网络安全市场规模将达 926.8 亿元，同比增长 23.7%[8]。2016-2021 年中国网络信息安全市场规模与增长如下图所示：



数据来源：赛迪咨询

[8]数据来源：赛迪咨询《2019 中国网络安全发展白皮书》

网络安全行业快速发展带动网络安全人才需求不断攀升。同时，伴随等保 2.0 的发布实施，中小型企业、私营企业等逐步设立网络安全专岗人员，人才需求量不断增加。2019 年上半年，我国政企机构对网络安全人才招聘规模环比增长 104.9%，网络安全人才教育需求旺盛，吸引越来越多的学生接受相关培训进入网络安全行业。2016-2019 年政企机构招聘网络安全岗位人才规模增长情况如下图所示：



数据来源：智联招聘

除在校学生外，网络空间安全教育的主要目标客户还包括具有继续学习需求的从业人员。《关键信息基础设施安全保护条例（征求意见稿）》的出台，更是让从业人员再培训转变为政策要求，《保护条例》第二十七条要求“运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于 1 个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于 3 个工作日。”法规的出台，释放出大量刚性网络安全教育需求。

我国网络安全行业的快速发展带动了人才教育、认证需求的增长，为本项目针对学生和在职人员的网络安全相关认证培训和非认证培训提供了广阔的市场空间，项目具有良好的市场可行性。

（3）公司的产品技术、人才和客户积累为本项目提供了实施可行性

公司在网络安全行业深耕多年，积累了行业领先的产品技术和人才基础，能够有效保障本项目顺利实施。

在产品技术方面，网络安全靶场产品主要运用的如虚拟网络构建、多维网络互联、能效评估分析、复杂虚拟化网络管理、可视化展现、异构虚拟化平台统一接入等技术是公司现有产品体系成熟技术，仅需针对教育场景进行研发转化。目

前公司已开展靶场产品开发工作并取得一定成果，为后续根据场景需要定制化开发有针对性的虚拟化技术、网络技术、虚实结合技术、数据分析算法等相关技术提供了良好的基础。

在人才积累方面，除网络安全专业技术人员外，公司在虚拟化技术开发、数据分析、靶场环境开发、网络安全培训、场景运维和教务等方面人员均有一定积累，能够有效保障项目的顺利实施。

目前，公司已为部分客户提供了靶场建设及定制服务，产品具备了一定的客户基础和品牌优势，为进一步客户拓展，扩大市场规模提供了有利条件。

（4）安恒信息具备颁发国家级认证证书的资质

安恒信息是最早一批联合中国信息安全测评中心认定的“授权培训机构”之一，也是目前浙江省唯一的一家 CISP 授权培训机构，可以为接受培训的合格学员提供注册大数据安全分析师（CISP-BDSA）、注册云安全工程师（CISP-CSE）认证资质。CISP 授权证书由中国信息安全测评中心组织和管理，是信息安全国内第一认证，在国内知名度最高、最受认可。此外，安恒信息还可以为合格学员提供注册 Web 安全工程师和注册工业控制系统安全工程师两大认证。

申请信息安全服务资质认证的厂商，根据申请的资质级别必须配备若干名具备 CISP 证书的人员。同时，拥有 CISP 人员的企业在参与政府、国企以及重点行业的招投标过程中具备竞争优势，网络安全厂商通常偏好招聘拥有 CISP 授权证书的求职人员。拥有颁发此项认证的资质是公司安全培训能力的有效背书，能够吸引更多潜在从业人员，有效提升公司开展网络安全云靶场研发及产业化项目的可行性。

5、投资概算

本项目预计建设期为 3 年，项目总投资 15,753.23 万元，拟投入募集资金 12,541.34 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**9,094.67**	**9,094.67**
1.1	场地建造费	6,190.57	6,190.57
1.2	硬件购置	1,953.10	1,953.10

1.3	软件购置	951.00	951.00
2	**研发费用**	**5,521.34**	**3,446.67**
3	**基本预备费 2%**	**292.32**	**-**
4	**铺底流动资金**	**844.90**	**-**
	合计	**15,753.23**	**12,541.34**

6、实施主体、项目选址和建设期限

本项目实施主体为安恒信息。项目拟在杭州市滨江区新建办公楼的部分楼层开展，预计建设期为 3 年。2020 年 7 月，公司已就项目建设所需用地与杭州市规划和自然资源局签署《国有建设用地使用权出让合同》。

7、项目备案和环评情况

截至本预案出具日，本项目的可行性研究报告已编制完毕，公司正在办理备案等相关事项。

8、项目经济效益评价

经测算，本项目税后内部收益率为 16.23%，税后静态投资回收期为 7.19 年，项目预期效益良好。

（五）新一代智能网关产品研发及产业化项目

1、项目概况

伴随国家网络强国战略和企业数字化转型的推进，有效保障网络信息安全，加快网络安全产品迭代的重要性愈发凸显。同时，云计算、大数据、物联网、工业互联网及人工智能等新兴技术的加速发展使得网络安全产品的应用环境日益复杂，数据泄露、高危漏洞等网络安全问题频发，对新一代网络安全产品综合协作能力的要求进一步提高，新一代网关产品进入技术更新迭代的关键窗口期，推动网关产品技术淘汰。公司拟把握新一代网关产品进入技术更新迭代关键窗口期的大好机遇，通过加大新一代智能网关产品研发，提升公司基础层安全产品水平，扩展产品市场份额。公司拟在成都购置办公场地开展新一代智能网关产品研发及产业化，并结合新场景将其适配应用于云计算、大数据、物联网、工业互联网及人工智能防护等新兴应用环境和技术方向，满足客户在新时代技术发展下数字化

转型的需求，提升公司综合安全解决方案的完整性和适配性，进一步扩大公司产品业务规模，提升整体竞争力。

2、项目建设内容

本项目新一代智能网关产品研发涉及矢量数据包转发技术、高性能报文分类匹配技术、入侵检测技术、防病毒技术、过滤技术、识别技术、联动技术和设备集中管控技术等，相关技术主要研发内容及在产品中的应用如下：

技术方向	主要研发内容	相关技术在产品中的应用
矢量数据包转发技术	高性能接口 IO 技术，报文零拷贝、报文高速解码、报文转发处理流程、高性能表项创建、查询、老化等技术研究	在网关设备中提供高性能、可扩展的报文处理机制，为数据转发引擎提供一个高性能的处理框架
高性能的报文分类匹配技术	数据包分类算法、多域网络数据包分类算法等匹配算法研究	在网关中通过该技术的研究提供高性能的报文匹配性能，提供网关的多维度的访问控制能力，如防火墙策略、NAT 策略。
入侵检测技术	入侵检测规则、入侵检测算法等技术研究	为网关提供入侵防御能力
防病毒技术	流式病毒检测技术、启发式病毒检测技术以及基于 AI 的神经网络病毒库训练以及识别等技术研究	为网关提供防病毒检测能力
URL 过滤技术	URL 分类技术以及 URL 高速匹配技术研究	提供网关在 URL 分类上的访问控制能力
内容过滤技术	流量基于不同协议以及不用应用的内容解析和匹配技术研究	提供网关在传输内容上的访问控制能力
应用识别技术	应用特征库、流量应用识别检测等技术研究	提供网关在应用上的访问控制能力
用户识别技术	用户管理、用户认证、用户访问控制以及用户流量统计等技术研究	提供网关在用户上的访问控制能力
DDOS 识别技术	开发多种 DDOS 攻击检测算法识别各种不同的 DDOS 攻击行为	提供 DDOS 攻击识别检测能力
IPv4/v6 双栈技术	IPv4/v6 双栈、过渡技术（nat64、dslite 等）等协议栈技术研究，	提供网关在 IPv4/v6 网络上的网络适配能力以及在过渡阶段的过渡技术
VPN 技术	L2tp、GRE、SSLVPN、IPsecVPN 等 VPN 技术研究	提供网关的分支互联组网以及外网安全接入的能力
联动技术	与其它安全产品的联动技术研究，如堡垒机、扫描器以及 EDR 等	提供网关支持各种层次的防护能力方案的能力
设备集中管控技术	设备的北向标准接口提供监控、配置管理以及接入授权等技术研究	提供设备第三方集成能力
威胁情报集成	集成安恒已有的数据大脑中的各种威胁情报数据，提高防护性能和防护准确性	提高安全防护检测能力
机器学习引擎	实现对流量、应用、文件、防护策略等多维度的机器建模，通过机器学习实现智能基线防护	提高安全防护检测能力

文件沙箱检测	集成沙箱检测能力，实现对文件的深度检测	提高安全防护检测能力
多安全防护平台集成	实现与运维网关、数据库安全防护网关、数据安全防护平台、EDR、态势感知、大数据智能分析平台等的集成	提供多种安全平台防护能力的无缝标准整合，提高安全防护检测能力
国产多硬件平台支持	解决多种国产化硬件平台的低成本支持，降低转发平面、安全检测防护引擎对硬件和内核等的过渡依赖	实现低成本支持多种硬件平台
云化支持	实现与硬件的解耦，便于通过与多云管理平台的集成，实现快速对多云环境的支持	提供多云快速云化部署能力
SSL 加速卡	实现对网络层加密流量的硬件加解密	提供加密流量的高性能加解密，提高整体防护性能
FPGA	解决部分基于正则表达式等特征策略的安全引擎靠 CPU 检测防护性能较低的问题，部分引擎移植到 FPGA 里面实现硬件层面快速高性能安全防护检测	提高安全引擎检测性能

3、项目必要性

（1）本项目有助于抓住行业技术迭代机遇，扩大公司网关产品业务规模

安全内容管理、防火墙、IDS/IPS、统一威胁管理、VPN 等五个细分市场构成了网络安全基础设施市场的主体。根据 IDC 统计数据，2019 年防火墙是我国网络安全基础设施市场占比最大细分市场，占比达 38%。目前同行业主要竞争对手中绿盟科技、奇安信、山石网科、天融信等在网络层防火墙领域均有较大的业务体量，且各主要安全厂商在 AI 防火墙层面的战略布局持续加深。公司初期基于业务规模限制，业务及技术主要聚焦于应用层安全领域，对网络基础层防护产品的研发投入有限，相关产品收入占比相对较低。2019 年度，公司基础网络层防护产品收入为 4,897.23 万元，仅占公司主营收入的 5.19%，与细分行业领先企业相比存在较大差距，潜力较大。

随着人工智能、区块链、5G、量子通信、工业互联网、大数据、云计算、物联网等具有颠覆性的战略性新技术快速演进，大规模数据泄露、高危漏洞、新技术应用下的网络攻击等网络安全问题频发，攻击团伙的智能化、商业化生态已形成，网络威胁态势严峻。在云计算、大数据、国产化替代及 AI 智能防护等需求的推动下，防火墙作为传统的网关产品处在向智能化、简易化及可视化方向技术更新迭代的关键阶段，市场现有产品技术架构受到挑战，行业竞争格局或将面临较大变动。

基于网关产品在整个网络安全防护产品市场中重要地位，公司拟研发新一代智能网关产品，抓住行业技术迭代的机遇，快速抢占扩大网关产品市场份额，本项目的顺利实施对扩大公司网络层安全业务规模、提升整体竞争实力意义重大。

（2）本项目有助于完善网络安全生态建设，推进整体解决方案集成联动

网络层网关防护技术在其他安全产品中有着广泛的应用，是构建网络安全生态建设必不可少的基础技术，尤其是数据中心出口以及云化场景，需要进行较大的改造集成，通过解决云环境流量牵引、控制防护平面解耦、安全能力集成、安全防护检测服务链等技术提升边界网关整体解决方案防护能力，形成整体安全防护产品的集成联动。自有基础层防护产品及技术的缺失将影响公司整体网络安全解决方案适配及稳定性。

基于公司业务整体发展和业绩提升考虑，本项目拟自建智能网关产品生产线，快速切入网络层防火墙、IPS 及 IDS 等网关市场，充分发挥公司在云计算安全、大数据安全、物联网安全及工业互联网安全等领域的技术积累，提升公司网关产品在相关领域的防护能力和适配能力，完善自有安全防护产品生态，提升整体解决方案能力。

4、项目可行性

（1）公司具备渠道和销售方面的优势，拥有良好的客户基础

公司自成立以来，始终专注于提供网络安全服务和解决方案，是全球网络安全创新 500 强之一。公司网络信息安全基础产品具有广泛的市场销量和客户基础，其中 Web 应用防火墙、数据库审计与风险控制系统、综合日志审计平台等产品处于行业领先位置。公司自 2017 年开始完善渠道建设，致力于加大渠道合作伙伴扶持力度、落实渠道激励政策，建设公司级的合作平台，并已形成成熟的行业直销和渠道代理销售模式。随着公司营销网络及渠道体系的不断完善，成熟的行业直销和渠道代理销售模式为本项目新一代智能网关产品的销售实现提供了可靠保障。

此外，公司作为网络安全综合解决方案提供商，整体产品体系具有较强联动性，公司将推动本项目新一代智能网关产品与自有云安全平台、大数据态势感知平台等集成整合，通过整体安全防护解决方案进一步带动产品销售。

（2）智能网关广阔的市场空间为本项目提供了市场保障

随着云计算、物联网、大数据、5G 等新兴技术的兴起，网络信息安全边界不断弱化，安全防护内容不断增加，对数据安全、信息安全提出了巨大挑战，迫使网络安全产品提升综合协作能力，推动网关等网络安全产品的技术更新迭代。根据赛迪顾问数据统计，到 2021 年网络安全市场规模将达到 1,648.9 亿美元。其中，防火墙作为最为通用的网络安全防御产品，根据 IDC 统计数据，2019 年防火墙是我国网络安全基础设施市场占比最大细分市场，占比达 38%。新兴技术的加速发展和应用环境的日益复杂推动网络安全市场规模不断增长，基于网关产品在国内网络安全市场的重要地位，新一代智能网关的市场空间广阔。本项目拟研发的新一代智能网关产品能够更好地适应日益复杂的应用环境，应用于“云计算、大数据、物联网、工业互联网、人工智能”等领域，为数字经济发展和企业数字化转型提供更全面、智能化的安全产品保障。

（3）公司丰富的技术积累为本项目提供了技术保障

本项目将开展高性能报文转发引擎、高性能安全检测引擎、协议处理引擎、安全防护引擎、多场景支持、硬件加速等部件的研发，具有较高的技术要求。截至 2020 年 9 月 30 日，公司拥有超过 130 项已获得授权的专利，对于项目所涉及的关键技术包括 DDOS 识别技术、VPN 技术、威胁情报集成技术、国产多硬件平台支持技术、云化支持技术等都已具备一定的研究基础，且部分研究成果已获得或正在申请专利授权。此外，公司目前在应用层有较多的安全防护检测能力及数据，能够有效助力新型智能网关产品研发，为项目提供技术保障。同时，公司已经在云安全、大数据安全、物联网安全及工业互联网安全等领域积累了丰富的技术和研发经验，为新一代智能网关产品在相关领域的研发与应用奠定了良好的技术基础。

5、投资概算

本项目预计建设期为 3 年，项目总投资 22,622.09 万元，拟投入募集资金 17,924.13 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额
1	**工程建设费用**	**13,948.79**	**13,948.79**

1.1	场地购置费	11,360.11	11,360.11
1.2	场地装修费	1,832.28	1,832.28
1.3	硬件购置	709.40	709.40
1.4	软件购置	47.00	47.00
2	**研发费用**	**6,368.25**	**3,975.34**
3	**基本预备费 2%**	**406.34**	-
4	**铺底流动资金**	**1,898.71**	-
	合计	**22,622.09**	**17,924.13**

6、实施主体、项目选址和建设期限

本项目实施主体为安恒信息全资子公司成都安恒信息技术有限公司。公司拟在成都购置办公场地开展新一代智能网关产品研发及产业化，预计建设期为 3 年。公司预计将于近期就本项目建设所需用楼签署购楼意向协议。

7、项目备案和环评情况

截至本预案出具日，本项目的可行性研究报告已编制完毕，公司正在办理备案等相关事项。

8、项目经济效益评价

经测算，本项目税后内部收益率为 24.50%，税后静态投资回收期为 5.82 年，项目预期效益良好。

（六）车联网安全研发中心建设项目

1、项目概况

为加快车联网（智能网联汽车）产业发展，2018 年 12 月工信部印发《车联网（智能网联汽车）产业发展行动计划》，要求从突破关键技术、完善标准体系、完善车联网产业基础设施、发展综合应用、完善安全保障体系等六个方面推动车联网产业发展。2019 年 9 月国务院印发《交通强国建设纲要》，要求进一步加强智能网联企业（智能汽车、自动驾驶、车路协同）研发，形成自主可控完整的产业链。随着 5G 时代的来临，5G 移动通信技术在提升峰值速率、移动性、时延和频谱效率等传统指标的基础上，还大幅提升了用户体验速率、连接数密度、流量密度和能效四个关键能力指标，能够有效满足车联网要求，5G 移动通信技

术的持续推进有望推动车联网的快速发展。公司作为专业的网络信息安全服务提供商，拟积极开展车联网安全技术研究，为车联网产业发展提供安全保障。

本项目拟建设车联网安全研发中心，进行车联网安全领域产品技术的研发。项目拟搭建完善的研发环境，引进行业专业人才，积极与整车厂商和科研院所合作，开展车联网安全产品体系的研发，为公司向车联网安全领域的业务拓展布局。

2、项目建设内容

车联网安全产品主要包括汽车安全检测中心、身份认证与应用安全、入侵检测与安全防护和 V2X 智能网联威胁分析平台等部分，系统架构及各部分主要功能如下：

①汽车安全检测中心：主要开展对于汽车安全的研究工作，为汽车安全的服务能力提升和产品研究发展提供坚实的技术基础。其包括汽车出厂生产安全检测服务、企业-联合安全研究所和高校-联合实训教学靶场三个部分。

②入侵检测与安全防护：主要侧重于智能网联车辆与外部数据交互的安全检测，保障车辆联网与数据交互安全。其包括车载入侵行为检测系统、OTA 升级安全检测以及 TSP 云端服务的安全体系建设，同时在端点测通过安全芯片的方式对各项安全能力进行应用移植，提高安全能力及应用效率。

③身份认证与应用安全：主要解决汽车联网过程中的身份可信问题，保障汽

车信息安全及行驶安全。其主要包括 PKI 和 KMS 系统，在基础车辆身份认证以及蓝牙钥匙、智能充电、智能租赁等众多新型智能网联车辆安全场景中广泛应用，同时也能够结合安全芯片提高整体验签性能与安全性。

④V2X-智能网联威胁分析平台：主要作用为分析整体车联网安全环境。从汽车威胁情报分析、V2X 汽车行驶安全和智慧交通安全等方面，结合网络安全探测、舆情能力和大数据分析建模能力，搭建汽车网络安全立体化分析中心。平台主要由车联网安全情报中心、汽车云端安全防护和智慧交通综合安全分析三个部分组成。

根据车联网安全产品功能特点及技术要求，本项目研发内容具体包括身份认证体系、车辆安全检测、靶场虚拟化技术、安全芯片应用、威胁情报获取和车载微流量监测技术，相关技术主要研发内容及在产品中的应用如下：

技术方向	主要研发内容	相关技术在产品中的应用
身份认证体系应用	国密算法加密、车辆身份标示、数字证书、密钥管理、快速认证。	在车联网身份认证及密钥管理平台中能对路边单元设备、智能网联汽车、TSP 云平台、移动手持设备等颁发唯一有效的许可证书，便于身份认证。
数据传输加密	数据传输加密算法及实现	在身份认证中提供可信支撑同时也为 V2X 环境下的数据交互提供保障
车辆安全检测	对于车辆软件、固件的安全分析及检测	形成专业化的检测能力与服务，为客户提供车辆安全检测的能力
车辆安全检测工具	将车辆安全检测能力进行固化、工具化	形成车辆安全检测的一体化工具，为车辆安全风险的高效检测提供专业支撑
安全芯片应用（车端的身份认证）	基于安全芯片的密钥管理，身份认证	秘钥管理，证书申请下载，boot 启动，校验，OTA 安全升级等安全功能
安全芯片应用（车路协同）	定制化密钥管理，身份认证，签名验签	OBU，RSU 和边缘设备上的可信任链建立，安全认证
安全芯片应用（入侵防护）	基于安全芯片的入侵防护技术，bootload 安全验证。	为车辆提供芯片级的入侵检测以及安全防护能力，硬件安全隔离
辅助驾驶系统安全模块	对于辅助驾驶系统中的关键输出指令数据进行模型分析	保障辅助驾驶系统的业务安全，信息安全，防止被网络攻击，确保车辆正常行驶
靶场虚拟化技术	将汽车应用场景进行虚拟化靶场搭建，形成可操作的高仿真靶场实验室	作为和高校间搭建联合实训教学靶场的技术基础，人才培养
威胁情报分析平台	对于网络中的车联网相关的情报信息获取	将获取到的情报信息整合后可以为客户或者是其他智慧交通类平台提供情报支撑
车载微流量监测技术	车内模块报文捕获、解析	为车辆入侵检测系统提供数据来源，数据入口

车辆安全风险检测能力	对于车内的报文指令信息进行分析，输出安全规则	为车辆入侵检测系统提供专业的安全规则，策略指令

3、项目必要性

（1）本项目有助于推动车联网安全保障体系的完善

车联网作为物联网在交通领域的典型应用，内容丰富，涉及面广。基于车联网“云”、“管”、“端”三层架构，车联网的网络安全重点关注智能网联汽车安全、移动智能终端安全、车联网服务平台安全、通信安全，同时数据安全和隐私保护贯穿于车联网的各个环节。随着车联网智能化和网联化的推进，车联网网络安全事件已然显现，根据 Upstream Security 发布的 2020 年《汽车网络安全报告》，汽车行业面临的网络威胁越来越普遍，自 2016 年以来发生的年安全事件数量增加了 605%。用户生命财产安全受到威胁，车联网安全已成为关系车联网发展的重要因素。2020 年 8 月工信部发布《关于开展 2020 年网络安全技术应用试点示范工作的通知》，将车联网安全列为重点方向。

本项目通过身份认证体系、车辆安全检测、靶场虚拟化技术、威胁情报获取和车载微流量技术的研发，能够进一步形成完善的车联网安全产品体系，满足车联网网络安全需求。凭借公司在网络信息安全领域成熟的产品技术，积极开展传统安全产品技术向车联网场景的研发转化，加强与车企客户和科研院所等在安全检测、验证、认证培训等方面的研发合作，推动公司车联网产业链的建设完善。本项目是公司顺应车联网产业发展的安全需求进行的产品技术研发，有助于推动车联网安全保障体系的建设完善。

（2）车联网明确的发展前景要求公司提前进行产品技术布局

2020 年是智能网联汽车行业政策和技术落地的关键节点。2019 年 9 月国务院发布《交通强国建设纲要》，明确提出加强智能网联汽车研发，形成自主可控完整的产业链。经过 2015-2019 年的前期重点培育，国内智能网联汽车行业逐步走向成熟，2020 年是智能网联企业行业落地的关键一年，国家对网联化水平确定了具体的考核指标，要求到 2020 年汽车 DA（驾驶辅助）、PA（部分自动驾驶）、CA（有条件自动驾驶）系统新车装配率超过 50%，网联式驾驶辅助系统装配率达到 10%；智能汽车新车占比达到 50%，中高级别智能汽车实现市场化应用，大城市、高速公路的车用无线通信网络（LTE-V2X）覆盖率达到 90%；

开展 5G-V2X 示范应用，车联网用户渗透率达到 30%以上，联网车载信息服务终端的新车装配率达到 60%以上。

在技术方面，5G 技术的发展有望推进智能网联汽车加速落地。5G 低延时、高可靠、大容量、大带宽及多并发数等特点有力支撑了车联网技术的发展，加速 T-Box 前装，加速动态数字地图更新，提高车载智能终端的渗透率和车路相关基础设施的通信能力。同时，V2X 技术路径之争逐步清晰。2019 年 12 月美国联邦通信委员会（FCC）通过了重新分配 5.9GHz 频段的 75MHz 频谱的提案，其中一部分频谱将用于 C-V2X 技术，C-V2X 技术地位逐步确立。2019 年 4 月，上汽、一汽、宇通等 13 家车企共同发布 C-V2X 商用路标，2020 下半年至 2021 上半年将陆续实现 C-V2X 汽车量产，2020 年是 C-V2X 产业化元年。

随着 V2X 技术路径的明确，在国家政策和 5G 商用的推动下，基于车联网在驾驶安全性和交通治理方面的突出优势，车联网发展前景进一步明确。目前我国已将车联网产业上升到国家战略高度，我国车联网产业化进程逐步加快，根据前瞻产业研究院发布的《中国车联网行业市场前瞻与投资战略规划分析报告》统计数据，截至 2017 年，全球车联网市场规模约为 525 亿美元，预计到 2022 年将增加至 1,629 亿美元，复合年均增长率为 25.4%；我国车联网市场规模将从 2017 年的 114 亿美元增长到 2022 年的 530 亿美元，复合年均增长率为 36.0%。本项目通过加强行业专业人才引进，开展车联网安全关键技术研发和储备，为公司未来拓展车联网安全业务提前进行产品技术布局。

（3）车联网应用新场景的拓展有利于进一步强化公司技术实力

车联网是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车与车、车与路边设施、车与行人以及车与网络之间进行无线通信和数据交换与共享的网络系统。与传统网络系统相比，车联网系统有着新的系统组成、新的通信场景，给系统安全性及用户隐私保护带来了新的挑战。

车联网是物联网技术应用的重要落地项目之一，也是建设智慧城市的重要组成部分，本项目关于车联网安全产品技术的研发将是公司物联网安全平台和智慧城市安全运营技术和解决方案的有效补充，有利于推动公司现有产品技术的完善，进一步强化公司技术实力。

4、项目可行性

（1）国家对网络安全及车联网安全的高度重视为行业发展提供了政策保障

网络安全政策法规的密集发布，彰显了政府对网络安全的高度重视。自 2019 年以来，国家在网络安全领域先后发布了《区块链信息服务管理规定》、《互联网个人信息安全保护指南》、网络安全等级保护制度 2.0 标准、《网络安全审查办法》、《数据安全管理办法（征求意见稿）》、《网络安全漏洞管理规定（征求意见稿）》、《云计算服务安全评估办法》、《加强工业互联网安全工作的指导意见》、《网络安全威胁信息发布管理办法（征求意见稿）》等政策法规，进一步加强了网络安全行业发展的顶层设计，明确了发展重点和方向，持续优化网络安全行业发展的政策环境。

此外车联网安全发展规划也在不断被提上日程，2018 年 12 月，工业和信息化部印发《车联网（智能网联汽车）产业发展行动计划》，将“强化管理、保障安全”作为基本要求，提出了“产业安全管理体系初步形成，安全管理制度与安全防护机制落地实施，安全技术及产品研发取得阶段性成果，安全技术支撑手段建设初见成效，安全保障和服务能力逐步完善”的阶段性发展目标。2020 年 2 月，国家发改委等部门在《智能汽车创新发展战略》中提出，到 2025 年，中国标准智能汽车的网络安全体系基本形成。国家对网络安全及车联网安全的高度重视为本项目提供了政策可行性。

（2）车联网广阔的市场空间为本项目提供了良好的发展前景

在政策和行业自然需求的推动下，传统汽车整体向智能网联发展已成确定趋势。由于我国汽车保有量巨大，在宏观政策、技术创新、基础设施建设等利好因素的影响下，新车搭载智能网联终端的比例将不断提高，预计 2025 年之前，大部分新车都将实现联网，同时联网汽车渗透率也将不断提升。而随着技术和服务的不断发展，汽车将成为继手机、电脑之后另一重要联网终端，不再局限于代步功能，服务内容的丰富也将推动用户对车联网功能付费意愿的提高，从而进一步提升市场空间。据赛迪顾问预测，预计到 2021 年我国车联网市场规模将达到 1,150 亿元，在 5G 技术推广应用、V2X 技术发展、用户增值付费提升等因素带动下，车联网市场将迎来爆发式增长。

由于车联网具有更复杂的网络系统，且其安全关系到车辆、行人和道路交通的整体安全，因此对车联网安全保障能力的要求较高，配置车联网安全产品成为网联智能汽车达到出厂标准的政策要求。全国汽车标准化技术委员会下属的智能网联汽车分技术委员会制定的《国家车联网产业标准体系建设指南（智能网联汽车）》中将信息安全标准体系（204）作为该标准的重要组成部分，提出“驾驶员或者车辆拥有者的个人隐私数据要保护；车辆运行信息向管理机构及用户有限度公开；针对信息交互建立相应的防护措施；针对信息防护失效建立应急处理机制”。此标准的制定意味着未来安装车联网安全产品将成为车辆符合汽车生产标准、通过汽车出厂安全检测的必要条件。

车联网安全已成为车联网行业发展的重要基础，车联网市场的快速增长将大幅带动车联网安全需求增长，本项目致力于开展车联网安全产品研发，具有良好的市场发展前景。

（3）公司丰富的技术积累和人才储备为本项目提供技术保障

公司立足车联网安全场景，积极开展与中国汽研等专业机构的研发合作。基于中国汽研在车辆检测领域的市场地位，与中国汽研的研发合作一方面能够保证本项目研发的产品技术贴近汽车安全检测标准，同时，也为后续车企客户拓展提供了便利。

公司现有丰富的网络信息安全技术及人才积累为项目实施提供了有效技术保障。公司在车联网安全领域的开发已取得阶段性成果：在车辆安全检测方面，随着与各大车企的深入合作，公司已经具备了提供完整安全服务和安全检测工具的能力；在车载网关方面，公司安全检测设备如 APT、IPS、WAF 等都已成熟，可在现有产品技术基础上结合车联网特定场景进行开发；公司针对车联网的 PKI 和 KMS 平台目前已基本开发完成，进入客户验证阶段。

5、投资概算

本项目预计建设期为 3 年，项目总投资 10,235.45 万元，拟投入募集资金 6,733.08 万元，其余所需资金通过自筹解决。项目具体投资内容如下：

单位：万元

序号	项目名称	投资总额	募集资金金额

1	**工程建设费用**	**1,248.00**	**1,248.00**
1.1	硬件购置	1,057.00	1,057.00
1.2	软件购置	191.00	191.00
2	**研发费用**	**8,786.75**	**5,485.08**
3	**基本预备费 2%**	**200.70**	**-**
	合计	**10,235.45**	**6,733.08**

6、实施主体、项目选址和建设期限

本项目实施主体为安恒信息。公司拟以现有办公场所安恒大厦为实施地点开展本项目，预计建设期为 3 年。

7、项目备案和环评情况

截至本预案出具日，本项目的可行性研究报告已编制完毕，公司正在办理备案等相关事项。

8、项目经济效益评价

本项目为研发项目，不直接产生收益。本项目效益体现在产品技术研发对公司未来业务发展提供技术支撑。

三、本次募集资金运用对公司财务状况及经营管理的影响

（一）对公司财务状况的影响

本次发行完成后，公司资产规模将大幅提高，资金实力显著提升，资产负债率下降，资产结构得到优化。

随着本次募集资金投资项目的开展，公司收入规模将持续上升，盈利能力得到提高，公司竞争实力进一步加强。

（二）对公司经营管理的影响

本次募集资金投资项目符合国家相关的产业政策以及未来公司整体战略发展方向，具有良好的市场发展前景和经济效益。其中，数据安全岛项目、涉网犯罪侦查打击项目、云靶场与教育产业化项目以及车联网安全项目系公司对网络安全领域新市场的开拓，有利于公司在横向上丰富产品结构，拓展业务布局，在相关领域掌握先发优势，抢占市场份额，提高行业地位。信创产业化项目及新一代

智能网关项目有助于公司快速响应客户对网络安全产品国产化适配以及新技术下智能网关产品的需求，抓住相关政策调整及产业发展机会，扩大公司产品业务规模，提升整体竞争力。

四、本次募集资金投资项目属于科技创新领域

（一）公司所处行业属于战略性新兴产业，科技创新属性突出

公司主营业务为信息安全产品的研发、生产及销售，并为客户提供专业的信息安全服务，公司研发人员占总人数比超过30%，研发投入占总收入比超过23%，是国家级高新技术企业。根据国家统计局颁布的《战略性新兴产业分类（2018）》，公司所处行业属于新一代信息技术产业——新兴软件和新型信息技术服务——网络与信息安全软件开发、互联网安全服务。同时，根据《上海证券交易所科创板企业上市推荐指引》第三条的规定，公司属于新一代信息技术、高端装备、新材料、新能源、节能环保以及生物医药等高新技术产业和战略性新兴产业的科技创新企业。

网络信息安全行业覆盖了网络通信、计算科学、数据应用、人工智能、密码技术、行为科学等众多技术领域。网络安全产业的范畴随着网络安全保障需求不断延伸扩展，要求网络安全公司不断开展研发创新，以满足大数据安全、云安全、物联网安全、工业互联网安全、威胁情报等细分市场对网络安全防护技术的新要求。在2016年启动的“十三五”国家科技创新规划中，国务院提出网络空间安全行业有良好的科创基础，属于需要进一步布局体现国家战略意图的重大科技项目。网络安全行业企业响应国家号召，不断加大科技创新力度，融合前沿科学技术创新网络安全产品，保障国家网络安全环境，行业战略政策地位进一步提升，科技创新属性突出。

（二）公司积极开展技术研发，重视科技创新能力

公司是网络信息安全行业领先企业，坚持技术创新的发展战略，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，大胆开拓新市场，产品在网络安全领域内拥有较强的竞争力。在网络安全基础产品领域，公司于成立之初便以应用安全和数据安全作为切入点，推出市场首创性产品数据库审计系统与Web应用防火墙产品，相关产品的市场份额位居市场前列。在网络安全平台和网

络安全服务领域，公司于2014年率先开始向云计算、大数据、物联网等新兴领域转型，贴合国内信息安全产业发展趋势，占据较大先发优势，拥有深厚的技术储备，相关业务已成为公司重要的营收增长点。

凭借研发团队多年的努力以及持续不断的研发投入，公司在产品技术上具有较强的研发能力，积累了丰富的研发和产业化密切结合的经验和雄厚的技术、专利储备。截至 2020 年 9 月 30 日，公司共拥有 48 项核心技术，拥有已授权专利超过 130 项。

（三）本次募投项目紧密围绕公司主营业务，促进公司科技创新能力提升

本次募投项目紧密围绕公司现有网络信息安全主营业务进行，募投项目与现有业务关联度高，是加强公司对前沿技术的研发、支撑行业应用的持续升级、深化公司在网络安全行业相关领域业务布局的重要举措。

其中，数据安全岛项目及涉网犯罪侦查打击项目在整合目前主营产品 AiLPHA 大数据智能安全平台以及态势感知预警平台的基础上拟进行数据隔离可信环境执行、安全计算沙箱、多方数据联合建模及案件线索主动发现等领域的研发，形成新的技术优势，为数字经济发展提供所需的安全保障；

信创产业化项目、云靶场与教育产业化项目及新一代智能网关项目是对公司现有产品及技术的适配改造及升级，以顺应当前国际局势与科技变革。面对国产化替代明确的发展趋势，公司拟依托其在网络安全领域的产品技术和人才基础，依据国家战略要求，对基础网络安全产品、云安全管控平台、态势感知平台和安全运营平台等进行国产化适配。基于国产化平台，全面开展信创领域的安全咨询、安全集成、安全运营等工作，加强对运维访问控制审计技术、分布式漏洞发现与验证技术、基于云架构的安全扫描与监测技术、SaaS 化云安全防护等技术的研发力度；本次云靶场与教育产业化项目通过网络安全靶场平台产品研发，加强现有网络安全产品向适用于教育教学产品的转化研发，为我国网络安全教学内容建设和网络安全人才培养提供实战化培训工具；新一代智能网关项目基于公司原有的应用层网关产品技术基础开发网络层网关产品，升级网关产品以适应云计算、大数据、人工智能等新兴技术发展下日益复杂的应用环境；

本次车联网安全研发项目拟通过身份认证体系、车辆安全检测、靶场虚拟化

技术、威胁情报获取和车载微流量技术的研发，凭借公司在网络信息安全领域成熟的产品技术将传统安全产品技术向车联网场景研发转化，形成完善的车联网安全产品体系，满足车联网网络安全需求，推动车联网产业链的建设完善。通过开展车联网安全关键技术研发和储备，为公司未来拓展车联网安全业务提前进行产品技术布局。

同时，本次募投项目中强调对研发项目的投入，募投项目的实施能够有效保障公司研发投入，储备科研资金，为公司的新产品及服务的研发和产业化实施提供必要的硬件设施与资金支持，为研发团队进行行业前沿研究提供更加优越的研发环境与条件，进一步提升研发在公司发展过程中的战略地位，促进公司科技创新水平提升。

综上所述，公司所处行业属于战略新兴行业，科技创新属性突出。公司在日常经营中积极开展研发工作，重视科技创新。本次募投项目紧密围绕公司主营业务开展，投向科技创新领域，待本次募集资金投资投产后，公司将实现业务板块的延伸和扩展，随着募投项目的实施及效益的产生，公司的技术盈利能力和经营业绩将进一步提升。

五、总结

本次向特定对象发行股票的募投项目建设有助于公司打造数据安全、涉网犯罪侦查打击、信创产业化、云靶场与教育产业化、新一代智能网关及车联网安全相关产品的研发和产业化实施平台，巩固公司技术优势，深化公司在相关网络安全细分领域的业务布局，提升公司竞争力，实现战略目标。

公司本次发行股票募集资金用于网络信息安全科技创新领域，募投项目紧密围绕公司现有网络信息安全主营业务进行，有利于公司科技创新实力的提升，符合《科创板上市公司证券发行注册管理办法（试行）》第十二条第（一）项的规定。本次向特定对象发行股票的募投项目建设符合中国相关产业政策和规划，符合公司的实际情况和战略需求。

第三节　董事会关于本次发行对公司影响的讨论与分析

一、发行后公司业务及资产整合计划

本次发行完成后，公司不存在较大的业务和资产的整合计划，本次发行均围绕公司现有主营业务展开，公司业务结构不会产生较大变化，公司的盈利能力将有所提升，主营业务将进一步加强。

二、发行后公司章程、股东结构、高管人员结构以及业务结构的变动情况

（一）发行后公司章程变动情况

本次发行完成后，公司的股本总额将有所上升，公司将根据股本的变化情况，履行《公司章程》修改的相关程序，对《公司章程》中与股本相关的条款进行相应的修改，并办理工商登记手续。除上述事项外，本次发行不会对公司章程造成影响。

（二）发行后上市公司股东结构变动情况

本次发行完成后，公司的股本规模、股东结构及持股比例将发生变化，本次发行不会导致公司控股股东及实际控制人发生变化。本次发行完成后，公司股权分布仍符合上市条件。

（三）高管人员结构变动情况

本次发行完成后，公司不会因本次发行而调整公司的高管人员。若公司拟调整高管人员结构，将根据有关规定，履行必要的法律程序和信息披露义务。

（四）公司业务结构变动情况

本次发行完成后，公司主营业务仍为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务，所处行业仍为网络信息安全行业，公司业务结构不会产生较大变化。

三、本次发行后上市公司财务状况、盈利能力及现金流量的变动情况

本次发行募集资金到位后，公司的总资产及净资产规模将相应增加，财务状况将得到改善，有利于优化公司的资产负债结构，增强公司核心竞争力，提高公司盈利能力。本次发行对公司财务状况、盈利能力及现金流量的具体影响如下：

（一）本次发行对公司财务状况的影响

本次发行完成后，公司的总资产及净资产规模将有所增长，资产负债结构将得到进一步优化，资本结构得到改善，公司整体财务状况得到提高，有利于增强公司抵御财务风险的能力，为公司的长期持续发展提供良好的保障。

（二）本次发行对公司盈利能力的影响

本次发行完成后，公司的总股本及净资产规模有所增加，但募集资金投资项目实施并产生效益需要一定周期。短期内，股本规模及净资产规模的扩大可能导致公司的每股收益被摊薄。

长期来看，本次向特定对象发行股票募集资金均用于公司的主营业务，募投项目与现有业务关联度高，是加强公司对前沿技术的研发、支撑行业应用的持续升级、深化公司在网络安全行业相关领域业务布局的重要举措。待本次募集资金投资投产后，公司将实现业务板块的延伸和扩展，随着募投项目的实施及效益的产生，公司的盈利能力和经营业绩将进一步提升。

（三）本次发行对公司现金流量的影响

本次发行后，随着募集资金的到位，公司筹资活动产生的现金流入将大幅增加；随着募集资金投资项目的实施及效益的产生，未来投资活动现金流出和经营活动现金流入将有所增加；随着公司盈利能力和经营状况的完善，公司整体现金流状况将得到进一步优化。

四、上市公司与控股股东、实际控制人及其关联人之间的业务关系、管理关系、同业竞争及关联交易等变化情况

（一）业务关系、管理关系的变化情况

公司是业务经营体系完整、人员配置完整的经济实体和企业法人，具有完全的自主经营权。本次发行前，公司在业务、人员、资产、机构、财务等方面均独立进行，不受控股股东及其关联人的影响。本次发行完成后，公司控股股东及实际控制人保持不变，公司与控股股东、实际控制人及其关联人之间的业务关系、管理关系均不存在重大变化。

（二）关联交易的变化情况

本次发行完成后，上市公司控股股东及实际控制人保持不变，上市公司与控股股东、实际控制人及其关联人之间的关联交易不存在重大变化。

（三）同业竞争的变化情况

本次发行完成前后，上市公司与控股股东、实际控制人及关联人之间不存在同业竞争的情况。

五、本次发行对公司资金、资产被控股股东及其关联人占用的影响，或对公司为控股股东及其关联人提供担保的影响

本次发行完成后，公司不存在资金、资产被控股股东及其关联人占用的情形，也不存在为控股股东及其关联人违规提供担保的情形。

六、本次发行对公司负债情况的影响

本次发行完成后，公司的资产负债率将有所下降，不存在通过本次发行大量增加负债（包括或有负债）的情况。公司的资产负债结构将更趋合理，抵御风险能力将进一步增强，符合公司全体股东的利益。

七、本次股票发行相关的风险说明

投资者在评价公司本次向特定对象发行股票时，除本预案提供的其他各项资料外，应特别认真考虑下述各项风险因素：

（一）对公司核心竞争力、经营稳定性及未来发展可能产生重大不利影响的因素

1、技术风险

（1）技术迭代风险

公司的核心技术主要应用于网络信息安全行业。随着信息技术的高速发展，网络信息安全领域的技术也伴随着处于快速成长期，应用的发展趋势表现为从搭载硬件的安全软件到提供云化网络信息安全保护、从传统数据保护到大数据保护、从互联网信息安全为主战场到物联网信息安全受到普遍重视、从分别提供安全软件和服务到提供整体安全解决方案等。进入该技术领域并将技术产业化需要长时间的研发积累和大量客户案例实践，技术壁垒和进入门槛较高。

如公司不能准确及时地预测和把握网络信息安全技术的发展趋势，对技术研究的路线做出合理安排或转型，在基础研究与市场应用上形成快速互动与良性循环，持续保持本公司技术领先优势，将可能会延缓本公司在关键技术和关键应用上实现突破的进度，导致本公司面临被竞争对手赶超，或者核心技术发展停滞甚至被替代的风险

（2）技术研发失败风险

网络信息安全行业是技术密集型行业。为保持市场领先优势，提升技术实力和核心竞争力，公司需要不断进行新技术创新、新产品研发，以应对终端客户日益增长的多样化需求。最近三年，公司的研发费用分别为9,592.94万元、15,195.19万元和20,453.95万元，占营业收入的比重分别为22.29%、24.25%和21.67%。发生的研发费用直接影响公司当年的净利润水平。由于对未来市场发展趋势的预测存在一定不确定性，公司可能面临新技术、新产品研发失败的风险，从而对公司

经营业绩和持续经营带来不利的影响。

（3）核心技术人员流失风险

经过多年积累和发展，公司形成了以核心技术人员为首的多个强有力的研发团队。核心技术人员是公司的核心竞争力及未来持续发展的基础。随着行业竞争日趋激烈，企业对人才的竞争不断加剧。能否维持技术人员队伍的稳定，并不断吸引优秀技术人员加盟，关系到公司能否继续保持技术竞争优势和未来发展的潜力。如果公司核心技术人员大量流失，则可能造成在研项目进度推迟、甚至终止，或者造成研发项目泄密或流失，给公司后续新产品的开发以及持续稳定增长带来不利影响。

2、经营风险

（1）市场竞争加剧的风险

我国网络信息安全行业市场空间已颇具规模，多年来保持了快速增长态势。市场机遇也吸引了较多参与者，市场竞争较为激烈。目前国内网络信息安全行业厂商众多，主营业务涵盖在网络信息安全的物理安全、网络安全、系统安全、应用安全、数据安全等多个细分领域中。未来，随着网络信息安全市场空间进一步拓展，公司与行业内具有技术、品牌、人才和资金优势的厂商之间的竞争可能进一步加剧。

（2）用户拓展失败的风险

网络信息安全危机事件频发，企业和社会民众对网络信息安全愈加重视，同时国家加强了政策对行业发展的引导和推动，行业下游客户范围逐步由政府（含公安）、金融机构、教育机构、电信运营商等单位向其他中小型企业覆盖，客户的需求也由产品需求增加了服务需求。公司目前客户群体主要集中在政府（含公安）、金融机构、教育机构、电信运营商等单位。公司计划加大营销网络建设方面的投入，建立多级销售渠道，以不断拓展中小企业客户，推广标准化网络信息安全产品，同时服务现有客户软件升级和新增业务的需要。但若公司的新行业拓展策略、营销服务等不能很好的适应并引导客户需求，公司将面临新行业市场开

拓风险。

（3）经营业绩季节性波动引起股价波动风险

公司报告期历年上半年营业收入较低，而下半年（特别是第四季度）营业收入较高，存在较为明显的季节性特征。

最近三年，公司营业收入按前三季度/四季度分布情况如下：

单位：万元

项目	2019 年度		2018 年度		2017 年度	
	金额	比例	金额	比例	金额	比例
前三季度	47,119.85	49.91%	31,042.77	49.54%	22,004.57	51.13%
第四季度	47,283.44	50.09%	31,615.90	50.46%	21,035.25	48.87%

受政府部门和大型企事业的采购周期影响，这些用户大多在上半年对全年的投资和采购进行规划，下半年再进行项目招标、项目验收和项目结算。同时，由于软件企业员工工资性支出、固定资产摊销等成本所占比重较高，造成公司净利润的季节性波动比营业收入的季节性波动更为明显。因此，公司经营业绩存在季节性波动引起股价波动风险。

（4）渠道商管理不善风险

报告期内，公司销售实行渠道加直销的销售模式，2017-2019 年度公司的渠道销售收入占营业收入的比重分别为 55.16%、55.93%和 58.26%，呈稳定上升趋势。公司产品具有客户集中度较低（2019 年前五大客户销售额占营业收入比为 15.59%，2020 年 1-9 月前五大客户销售额占营业收入比为 14.85%）、产品的目标用户数多、用户的地域及行业分布广的特点。随着未来公司经营规模的继续扩大，渠道管理的难度也将加大，若公司不能及时提高渠道管理能力，可能对公司品牌和产品销售造成不利影响。

（5）因最终客户发生数据泄密及其他网络安全事件时，公司承担罚款或赔偿的风险

当最终客户发生数据泄密及其他网络安全事件时，如主管部门认定公司在提供相应产品或服务时违反了国家与网络安全和信息安全相关的法律法规，公司可能承担相应的法律责任，并可能需根据销售合同的约定向客户承担相应的赔偿责任，从而给公司的经营带来一定风险。

3、行业风险

我国网络信息安全行业多年来保持了快速增长态势。市场机遇吸引了较多参与者，市场竞争较为激烈。未来，随着网络信息安全行业的发展，不同细分领域的技术将会融合、协同，不同细分市场客户的需求将会交叉、重叠，不同细分行业的领先者将展开直接竞争，行业的发展对公司提供整体解决方案的能力将提出更高的要求，公司与行业内具有技术、品牌、人才和资金优势的厂商之间的竞争可能进一步加剧，行业内目前的主要参与者也将面临具有新一代信息技术优势的企业可能进入网络信息安全行业的潜在竞争，行业整体竞争加剧可能影响行业总体毛利率，从而导致公司毛利率存在下降的风险。

同时，公司所处的信息安全行业未来保持快速发展的趋势基于目前国家政策取向、全球信息安全形势和未来技术发展方向，这些因素共同推动我国政府和企业不断增加对信息安全产品和服务的购买。一旦外部因素发生重大变化，或者政府和企业的购买偏好发生变化，就可能会导致信息安全行业发展不及预期，进而影响公司业绩。

4、法律风险

（1）相关业务和产品资质证书续期或办理风险

网络信息安全及网络设备厂商从事研发、生产、销售和提供安全服务等经营活动，通常需取得计算机信息系统安全专用产品销售许可证等产品认证，并具备网络信息安全服务资质等业务资质。截至立项报告出具日，公司拥有 IT 产品信息安全产品认证证书、中国国家信息安全产品认证证书、信息技术产品安全测评证书、计算机信息系统安全专用产品销售许可证、信息安全服务资质认证证书、中国通信企业协会通信网络安全服务能力评定证书、信息安全等级保护安全建设

服务机构能力评估合格证书等信息安全行业的主要产品和服务资质证书。虽然公司内部有专人负责产品和服务认证的申请、取得和维护，且未曾出现过已取得认证或资质被取消的情况，但如果未来国家关于产品和服务认证的政策或标准出现重大变化，公司无法为过期证书续证，产品和服务存在不能获得相关认证的风险。

5、财务风险

（1）应收账款大幅增加未来发生坏账的风险

截至 2020 年 9 月 30 日，公司应收账款余额为 23,936.79 万元，占资产总额 11.91%，应收账款规模较大。2019 年末应收账款余额较 2018 年末应收账款余额增加 19.26%，2018 年末应收账款余额较 2017 年末应收账款余额增长 52.46%。

随着业务规模的不断增长，公司每年实现销售的客户数量逐年扩大、市场区域不断扩大、客户类型继续增加，公司对客户的信用管理难度将增大，未来坏账风险可能增加。

6、政策风险

（1）税收优惠依赖风险

报告期内，公司享受的主要税收优惠政策包括：一是公司销售自主开发的软件产品增值税实际税负超过 3%的部分实行即征即退政策，二是公司作为国家规划布局内重点软件企业享受企业所得税 10%的优惠税率。

公司享受的税收优惠均与公司日常经营相关，具有一定的稳定性和持续性。2017-2019 年度公司实现收入 43,039.81 万元、62,658.68 万元及 94,403.29 万元，随着销售规模的快速增长，公司享受的税收优惠金额也逐步增加。

如果公司未来不能持续保持较强的盈利能力或者国家税收政策发生变动，则可能对公司利润水平产生一定的影响。

（2）财政补贴变化产生的风险

报告期内，政府一直重视高新技术企业，并给予重点鼓励和扶持。报告期内，

公司除增值税退税外政府补助收入分别为 1,508.04 万元、1,554.28 万元、1,507.60 万元及 1,543.11 万元。补助项目包括安恒信息智慧安全云省级重点企业研究院项目补助资金等。如果政府对公司所处行业及高新技术企业的扶持政策发生变化，将对公司的发展产生一定的影响。

7、新冠肺炎疫情带来的风险

自2020年初新冠肺炎疫情发生以来，受经济活动减弱、人口流动减少或延后、企业大范围停工停产等因素的影响，公司业务受到一定程度的冲击，2020年度上半年业绩增速较过往年度相比有所放缓。随着疫情情况得到基本控制，公司各项经营活动已基本恢复正常。但如果此次疫情发展趋势发生重大不利变化，或者在后续经营中再次遇到重大疫情、自然灾害或极端恶劣天气的影响，则可能对公司的日常经营和本次募投项目的实施造成不利影响。

（二）可能导致本次发行失败或募集资金不足的因素

1、审批风险

本次发行尚需满足多项条件方可完成，包括但不限于公司股东大会批准本次发行、上海证券交易所审核通过并获得中国证监会注册等。本次发行能否获得上述批准或注册，以及获得相关批准或注册的时间均存在不确定性，提请广大投资者注意投资风险。

2、发行风险

本次发行的发行对象为不超过 35 名（含 35 名）的特定对象，且最终根据竞价结果与本次发行的保荐机构（主承销商）协商确定，发行价格不低于定价基准日（即发行期首日）前二十个交易日公司 A 股股票交易均价的百分之八十。

本次发行的发行结果将受到宏观经济和行业发展情况、证券市场整体情况、公司股票价格走势、投资者对本次发行方案的认可程度等多种内外部因素的影响。

因此，本次发行存在发行募集资金不足甚至无法成功实施的风险

（三）对本次募投项目的实施过程或实施效果可能产生重大不利影响的因素

1、募集资金投资项目实施的风险

公司按照自身战略规划，围绕数据安全、涉网犯罪侦查打击、信创产业化、云靶场与教育产业化、新一代智能网关及车联网安全等方向设立募投项目，在现有网络信息安全产品及服务体系基础上进一步升级和拓展。公司已就本次拟实施募投项目进行了充分的市场调研和严格的可行性论证，并与部分客户签订意向订单或战略合作协议。但是由于本次募集资金投资项目均系公司新晋研发方向，在后续研发过程中有可能出现一些不可控因素或目前技术条件下尚不能解决的技术问题，导致研发进度不及预期或失败。同时，网络安全行业景气度受国家产业政策、政府宏观调控影响较大，若上述因素出现不可预见的负面变化，将对募投项目的效益实现产生较大影响。基于上述情况，本次募投项目存在无法及时、充分实施或难以达到预期经济效益的风险。

2、募投项目无法达到预期收益的风险

公司募集资金项目的可行性研究是基于当前经济形势、行业发展趋势、未来市场需求预测、公司技术研发能力等因素提出，公司经审慎测算后认为本次募集投资项目预期经济效益良好。但是考虑未来的经济形势、行业发展趋势、市场竞争环境等存在不确定性，以及项目实施风险（成本增加、进度延迟、募集资金不能及时到位等）和人员工资可能上升等因素，有可能导致募集资金投资项目的实际效益不及预期。

第四节　公司利润分配政策和执行情况

一、利润分配政策

为完善和健全科学、持续和稳定的股东回报机制，增加利润分配政策的透明度和可操作性，切实保护公众投资者的合法权益，根据中国证监会《上市公司监管指引第 3 号——上市公司现金分红》（证监会公告〔2013〕43 号）、《关于进一步落实上市公司现金分红有关事项的通知》（证监发〔2012〕37 号）、《上海证券交易所上市公司现金分红指引》的相关规定，公司已有完善的股利分配政策，在《公司章程》中制定了有关利润分配和现金分红政策如下：

（一）利润分配原则

公司实行稳定、持续、合理的利润分配政策，重视对投资者的合理回报并兼顾公司的可持续发展，每年将根据当期的经营情况和项目投资的资金需求计划，在充分考虑股东利益的基础上正确处理公司的短期利益与长远发展的关系，充分听取股东（特别是中小股东）、独立董事和监事的意见，确定合理的利润分配方案。

（二）利润分配形式

公司采用现金、股票或者现金与股票相结合的方式分配利润，利润分配不得超过累计可分配利润的范围，不得损害公司持续经营能力。在当年盈利的条件下，且在无重大投资计划或重大现金支出发生时，公司应当优先采用现金方式分配股利。

（三）现金分红的具体条件和比例

1、现金分红的期间间隔

公司在具备利润分配条件的情况下，原则上每年度进行一次现金分红，公司董事会可以根据公司盈利及资金需求情况提议公司进行中期现金分红。

2、现金分红的具体条件

除公司有重大投资计划或重大现金支出安排外，在公司当年盈利、累计未分配利润为正值且满足公司正常生产经营的资金需求情况下，公司应当采取现金方式分配股利。重大投资计划或重大现金支出安排是指公司未来 12 个月内购买资产、对外投资、进行固定资产投资等交易累计支出达到或超过公司最近一期经审计净资产 30%。

3、现金分红的比例

公司任何三个连续年度内，公司以现金方式累计分配的利润应当不少于该三年公司实现的年均可分配利润的 30%。具体每个年度的分红比例由董事会根据公司年度盈利状况和未来资金使用计划或规划综合分析权衡后提出预案。

公司董事会应当综合考虑所处行业特点、发展阶段、自身经营模式、盈利水平以及是否有重大资金支出安排等因素，区分下列情形，并按照公司章程规定的程序，提出差异化的现金分红政策：

1）公司发展阶段属成熟期且无重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 80%；

2）公司发展阶段属成熟期且有重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 40%；

3）公司发展阶段属成长期且有重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 20%；

4）公司发展阶段不易区分但有重大资金支出安排的，可以按照前项规定处理。

（四）发放股票股利的具体条件

公司在经营情况良好，并且董事会认为公司股票价格与公司股本规模不匹配、发放股票股利有利于公司全体股东整体利益时，可以在满足上述现金分红的条件下，提出股票股利分配方案。

（五）利润分配的决策程序与机制

1、利润分配方案的拟定

董事会结合公司章程的规定和经营状况，与独立董事、监事充分讨论，充分考虑中小股东的意见，在考虑对全体股东持续、稳定、科学的回报基础上形成利润分配方案。独立董事应当发表独立意见，独立董事可以征集中小股东的意见，提出分红提案，并提交董事会审议。

2、利润分配的决策程序

（1）董事会在审议利润分配方案时，应当认真研究和论证公司现金分红的时机、条件和比例、调整的条件等事宜，应充分听取监事会的意见，独立董事应发表明确意见。

（2）利润分配方案经董事会、监事会审议通过后提交股东大会进行审议。股东大会对现金分红具体方案进行审议前，公司应当通过多种渠道主动与股东特别是中小股东进行沟通和交流，充分听取中小股东的意见和诉求，及时答复中小股东关心的问题。

（3）公司因前述规定的特殊情况而不进行现金分红时，董事会就不进行现金分红的具体原因、公司留存收益的确切用途及预计投资收益等事项进行专项说明，经独立董事发表意见后提交股东大会审议。

（六）利润分配政策的调整或变更的决策机制与程序

公司因生产经营情况发生重大变化、投资规划和长期发展的需要等原因需调整利润分配政策的，应由公司董事会根据实际情况提出利润分配政策调整议案，调整后的利润分配政策应以股东权益保护为出发点，且不得违反中国证监会和证券交易所的有关规定；独立董事、监事会应当对调整利润分配政策发表审核意见，并由出席股东大会的股东所持表决权的 2/3 以上通过。

二、公司近三年的现金分红及利润分配政策执行情况

公司自2019年11月5日上市以来，严格按照公司章程的规定向公司股东分配股利。2020年5月7日，公司召开的2019年度股东大会审议通过了《关于公司2019年度利润分配方案的议案》，以总股本74,074,075股为基数，每股派发现金红利0.378元（含税），共计派发现金红利2,800.00万元，不送红股，不以公积金转增股本，剩余未分配利润结转下一年度。公司最近三年现金股利分配情况如下：

单位：万元

项目	2019年	2018年	2017年
合并报表中归属于上市公司股东的净利润	9,222.04	7,687.47	5,213.53
现金分红（含税）	2,800.00	-	-
当年现金分红占归属上市公司股东的净利润的比例	30.36%	-	-
最近三年累计现金分配利润占年均归属于上市公司股东的净利润比例	37.97%		

三、公司未来三年股东回报规划

公司为明确对新老股东合理投资回报，增加利润分配决策透明度和可操作性，便于股东对公司经营和利润分配进行监督，制定了《杭州安恒信息技术股份有限公司关于未来三年（2020 年-2022 年）股东分红回报规划》，主要内容如下：

为明确杭州安恒信息技术股份有限公司（以下简称“公司”）未来三年（2020 年-2022 年）股东回报规划，公司根据中国证券监督管理委员会《关于修改上市公司现金分红若干规定的决定》（证监会令第 57 号）、《关于进一步落实上市公司现金分红有关事项的通知》（证监发[2012]37 号）、《上市公司监管指引第 3 号—上市公司现金分红》（证监会公告[2013]43 号）、《上海证券交易所科创板股票上市规则》（上证发[2019]22 号）、《上海证券交易所上市公司现金分红指引》（上证公字[2013]1 号）及《杭州安恒信息技术股份有限公司章程》（以下简称《公司章程》”）的相关规定，制定《杭州安恒信息技术股份有限公司未来三年（2020 年-2022 年）股东回报规划》（以下简称“《规划》”），本《规划》具体内容如下：

（一）公司分红回报规划考虑因素

公司着眼于长远和可持续发展，在综合考虑企业经营发展实际、股东意愿和外部融资环境等因素的基础上，对利润分配作出制度性安排，从而建立对投资者

持续、稳定、科学的分红回报机制，以保证公司股利分配的连续性和稳定性。

（二）公司分红回报规划制定原则

1、公司充分考虑对投资者的回报，以最近三年现金方式累计分配的利润不少于最近三年实现的年均可分配利润的 30%的方式向股东分配股利；

2、公司的利润分配政策保持连续性和稳定性，同时兼顾公司的长远利益、全体股东的整体利益及公司的可持续发展；

3、公司优先采用现金方式分配股利。

（三）公司利润分配的顺序

公司当年税后利润，按下列顺序分配：

1、弥补以往年度的亏损；

2、提取利润的百分之十列入公司法定公积金；

3、提取任意公积金；

4、支付股东股利。

公司法定公积金累计达到公司注册资本的百分之五十以上的，可以不再提取。提取法定公积金后，是否提取任意公积金由股东大会决定。公司在弥补公司亏损、提取法定公积金前不向股东分配利润。

股东大会违反前款规定，在公司弥补亏损和提取法定公积金前向股东分配利润的，股东必须将违反规定分配的利润退还公司。

公司弥补亏损和提取公积金后所余税后利润，按照股东持有的股份比例分配，但公司章程规定不按持股比例分配的除外。

公司持有的本公司股份不参与分配利润。公司弥补亏损和提取法定公积金之前向股东分配利润的，股东必须将违反规定分配的利润退还公司。

（四）公司未来分红回报的具体政策

1、利润分配的形式：公司采用现金、股票或者现金与股票相结合的方式分配股利，优先采用现金分红的方式进行利润分配。公司在具备利润分配条件的情况下，原则上每年度进行一次现金分红。在有条件的情况下，公司可以进行中期利润分配。

2、公司以现金方式分配股利的具体条件和比例：除下述特殊情况不进行现金方式分配股利外，公司在当年盈利且累计未分配利润为正的情况下，采取现金方式分配股利：

（1）公司未来十二个月内有重大投资计划或重大现金支出（募集资金项目除外）；

（2）公司当年经审计资产负债率（母公司）超过 70%；

（3）公司当年实现的每股可供分配利润少于 0.1 元。

重大投资计划或重大现金支出是指，公司拟对外投资、收购资产或者购买设备的累计支出达到或者超过公司最近一期经审计的合并报表净资产的 30%。

3、公司应当综合考虑所处行业特点、发展阶段、自身经营模式、盈利水平以及是否有重大资金支出安排等因素，由董事会根据下列情形，提出差异化的现金分红方案，并提交股东大会批准：

（1）公司发展阶段属成熟期且无重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 80%；

（2）公司发展阶段属成熟期且有重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 40%；

（3）公司发展阶段属成长期且有重大资金支出安排的，进行利润分配时，现金分红在本次利润分配中所占比例最低应达到 20%；

（4）公司发展阶段不易区分但有重大资金支出安排的，可以按照前项规定

处理。

4、公司发放股票股利的具体条件：

在保证公司股本规模和股权结构合理的前提下，基于回报投资者和分享公司价值的考虑，从公司成长性、每股净资产的摊薄、公司股价与公司股本规模的匹配性等真实因素出发，当公司股票估值处于合理范围内，公司可以在在满足上述现金股利分配的条件下，进行股票股利分配。

（五）公司未来分红回报的决策和实施

1、利润分配方案的拟定。董事会结合公司章程的规定和经营状况，与独立董事、监事充分讨论，充分考虑中小股东的意见，在考虑对全体股东持续、稳定、科学的回报基础上形成利润分配方案。独立董事应当发表独立意见，独立董事可以征集中小股东的意见，提出分红提案，并提交董事会审议。

2、利润分配的决策程序。董事会审议利润分配方案时应当认真研究和论证公司现金分红的时机、条件和最低比例，调整的条件及其决策程序要求等事宜，就利润分配方案的合理性进行充分讨论。利润分配方案须经全体董事过半数表决同意，且经公司二分之一以上独立董事表决同意并发表明确独立意见。独立董事可以征集中小股东的意见，提出分红提案，并直接提交董事会审议。监事会应对董事会制订的利润分配方案进行审核并发表审核意见。

董事会审议通过利润分配方案后，应提交股东大会审议批准。公司公告董事会决议时应同时披露独立董事和监事会的审核意见，方能提交公司股东大会审议。股东大会审议利润分配方案时，公司应通过提供网络投票等方式切实保障社会公众股股东参与股东大会的权利。

股东大会对现金分红具体方案进行审议前，公司应当通过接听投资者电话、公司公共邮箱、网络平台、召开投资者见面会等多种渠道主动与股东特别是中小股东进行沟通和交流，充分听取中小股东的意见和诉求，及时答复中小股东关心的问题。

现金利润分配方案应经出席股东大会的股东所持表决权的二分之一以上通过，股票股利分配方案应经出席股东大会的股东所持表决权的三分之二以上通过。

3、公司因出现前述规定的特殊情况而不按规定进行现金股利分配时，董事会应就其具体原因、公司留存收益的确切用途及预计投资收益等事项进行专项说明，经独立董事发表明确意见后提交股东大会审议，并在公司指定媒体上予以披露。

4、公司股东大会审议通过利润分配决议后的 2 个月内，董事会必须完成股利（或股份）的派发事项。

（六）股东未来分红回报规划的变更

1、公司应以三年为周期，根据《公司章程》修订《股东未来分红回报规划》。

2、如遇到战争、自然灾害等不可抗力事件，并对公司生产经营造成重大影响，或者公司自身经营状况发生重大变化时，公司可对利润分配政策进行调整。

公司调整利润分配方案，必须由董事会进行专项讨论，详细论证说明理由，并将书面论证报告经独立董事同意后，提交股东大会并经出席股东大会的股东所持表决权的三分之二以上通过。

股东大会审议利润分配政策变更事项时，必须提供网络投票方式。

（七）其他

公司最近三年以现金方式累计分配的利润少于最近三年实现的年均可分配利润的 30%的，不得向社会公众增发新股、发行可转换公司债券或向原有股东配售股份。

股东违规占用公司资金情况的，公司应当扣减该股东本应分配的现金股利，以偿还其占用的资金。

第五节　本次向特定对象发行股票摊薄即期回报分析

根据《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）和《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（中国证券监督管理委员会公告[2015]31 号）要求，公司就本次发行对即期回报摊薄的影响进行了认真分析，并就本次发行摊薄即期回报对公司主要财务指标的影响及公司采取的措施分析如下：

一、本次发行对公司主要财务指标的影响

（一）财务指标计算的主要假设和前提

1、假设宏观经济环境及公司所处行业未发生重大不利变化。

2、假设本次发行于 2021 年 6 月底完成发行，该完成时间仅用于计算本次向特定对象发行 A 股股票对摊薄即期回报的影响，最终完成时间以经证监会同意注册并实际发行完成时间为准。

3、假设本次向特定对象发行股票数量为 22,222,222 股。若公司在本次向特定对象发行 A 股股票的定价基准日至发行日期间发生送股、回购、资本公积金转增股本等股本变动事项，本次向特定对象发行股票的发行数量将进行相应调整。

4、2019 年和 2020 年度，公司在前三季度分别实现营业收入 47,119.85 万元和 66,020.92 万元。2019 年公司营业收入为 94,403.29 万元，归属于母公司股东的净利润和扣除非经常性损益后归属于母公司股东的净利润分别为 9,222.04 万元和 7,959.44 万元，以此计算得出归属于母公司股东的净利率和扣除非经常性损益后归属于母公司股东的净利率分别为 9.77%和 8.43%。假设公司 2020 年度年归属于母公司所有者的净利润=2019 年度营业收入*（2020 年度前三季度收入/2019 年度前三季度收入）*2019 年度归属于母公司股东的净利率，公司 2020 年度扣除非经常性损益后归属于母公司股东的净利润=2019 年度营业收入*（2020 年度前三季度收入/2019 年度前三季度收入）*2019 年度扣除非经常性损益后归

属于母公司股东的净利率。

假设 2021 年度归属于母公司所有者的预测净利润及扣除非经常损益的预测净利润在 2020 年基础上按照增长 10%、增长 20%、增长 30%三种情景分别计算（上述增长率不代表公司对未来利润的盈利预测，仅用于计算本次发行摊薄即期回报对主要指标的影响）。

5、本测算未考虑本次发行募集资金到账后，对公司生产经营、财务状况（如财务费用、投资收益）等的影响。

6、假设除本次发行及上述事项外，公司未实施其他会对公司总股本发生影响或潜在影响的行为。

以上仅为基于测算目的假设，不构成承诺及盈利预测和业绩承诺，投资者不应据此假设进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。

（二）对公司主要财务指标的影响

基于上述假设，公司测算了本次发行摊薄即期回报对每股收益的影响，具体情况如下：

项目	2020 年度/2020 年 12 月 31 日	2021 年度/2021 年 12 月 31 日	
		本次发行前	本次发行后
总股本（股）	74,074,075	74,074,075	96,296,297
假设情形（1）：2021 年净利润较 2020 年增长 10%			
归属于母公司股东的净利润（万元）	12,921.26	14,213.39	14,213.39
扣除非经常性损益后归属于母公司股东的净利润（万元）	11,152.19	12,267.40	12,267.40
基本每股收益（元/股）	1.74	1.92	1.67
稀释每股收益（元/股）	1.74	1.92	1.67
扣除非经常性损益后基本每股收益（元/股）	1.51	1.66	1.44
扣除非经常性损益后稀释每股收益（元/股）	1.51	1.66	1.44
假设情形（2）：2021 年净利润较 2020 年增长 20%			

归属于母公司股东的净利润（万元）	12,921.26	15,505.51	15,505.51
扣除非经常性损益后归属于母公司股东的净利润（万元）	11,152.19	13,382.62	13,382.62
基本每股收益（元/股）	1.74	2.09	1.82
稀释每股收益（元/股）	1.74	2.09	1.82
扣除非经常性损益后基本每股收益（元/股）	1.51	1.81	1.57
扣除非经常性损益后稀释每股收益（元/股）	1.51	1.81	1.57
假设情形（3）：2021 年净利润较 2020 年增长 30%			
归属于母公司股东的净利润（万元）	12,921.26	16,797.64	16,797.64
扣除非经常性损益后归属于母公司股东的净利润（万元）	11,152.19	14,497.84	14,497.84
基本每股收益（元/股）	1.74	2.27	1.97
稀释每股收益（元/股）	1.74	2.27	1.97
扣除非经常性损益后基本每股收益（元/股）	1.51	1.96	1.70
扣除非经常性损益后稀释每股收益（元/股）	1.51	1.96	1.70

注：

1、上述测算未考虑本次发行募集资金到账后，对公司经营情况的影响。

2、基本每股收益、稀释每股收益系按照《公开发行证券的公司信息披露编报规则第 9 号——净资产收益率和每股收益的计算及披露》（2010 年修订）规定测算。

本次发行完成后，预计短期内公司基本每股收益、稀释每股收益将可能出现一定程度的下降，因此，公司短期内即期回报可能会出现一定程度摊薄。

二、本次向特定对象发行股票摊薄即期回报的风险提示

本次发行完成后，随着募集资金到位，公司净资产将会大幅增加，而本次募集资金投资项目效益的实现需要一定时间，若公司利润短期内不能得到相应幅度的增加，公司的每股收益和净资产收益率等指标将出现一定幅度的下降的可能性，公司股东即期回报存在被摊薄的风险。

此外，一旦前述分析的假设条件或公司经营发生重大变化，不能排除本次发

行导致即期回报被摊薄情况发生变化的可能性。特此提醒投资者关注本次发行可能摊薄即期回报的风险。

同时，在测算本次发行对即期回报的摊薄影响过程中，公司对 2020 年度、2021 年度归属于上市公司所有者的净利润的假设分析并非公司的盈利预测，为应对即期回报被摊薄风险而制定的填补回报具体措施不等于对公司未来利润做出保证，投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。提请广大投资者注意。

三、本次向特定对象发行股票的必要性和合理性

（一）符合公司发展战略需求

软件与信息技术服务行业技术升级与产品更新换代迅速，企业必须根据市场发展把握创新方向，持续不断的加大研发投入、推进技术创新以及新产品开发，并将创新成果转化为成熟产品推向市场，以适应不断发展的市场需求。

公司自成立以来一直专注于网络安全行业，已成长为国内网络信息安全领域的龙头企业。本次募集资金投资项目建成后，公司业务布局向数据安全、涉网犯罪侦查打击、信创产业化、云靶场与教育产业化、车联网安全等多个应用领域深化发展，公司安全整体解决方案更趋完善。本次募集资金投资项目符合国家产业政策和公司整体经营发展战略，具有良好的市场前景和综合效益，有利于公司开拓新兴市场，提升服务能力，增强公司核心竞争力，保障公司业务持续健康发展。

（二）为业务发展提供资金支持

作为高科技企业，公司具有高研发投入的特点，公司所从事的行业技术密集度较高，要保持公司的核心竞争力，就必须坚持研发创新投入。公司缺少满足银行要求的抵押物，传统贷款融资的能力受到一定限制。同时，公司面向的企业级客户一般采取预算制，且部分行业客户的投资来自于财政拨款，宏观经济环境的波动可能影响部分行业客户的 IT 投资预算，进而可能对公司的业务产生一定影响。因此，公司需要通过股权融资方式，增强资金实力，提高公司的抗风险能力。

（三）有利于优化公司资本结构

如果公司通过银行贷款等债务融资方式募集资金，将会导致公司资产负债率大幅提高，进而增加公司财务风险，不利于公司的稳健经营。通过本次发行股票募集资金，公司的总资产及净资产规模均相应增加，进一步增强资金实力，为后续发展提供有力保障；同时，有效降低资产负债率，促进公司的稳健经营，增强抵御财务风险的能力。

四、本次募集资金投资项目与公司现有业务的关系，公司从事募投项目在人员、技术、市场等方面的储备情况

（一）本次募集资金投资项目与公司现有业务的关系

公司自设立以来一直专注于网络信息安全领域，主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。公司的产品及服务涉及应用安全、云安全、大数据安全、物联网安全、智慧城市安全和工业互联网安全等领域。

本次募集资金投资项目围绕公司主营业务开展，结合大数据、云计算、物联网等新兴技术，针对数据安全、涉网犯罪侦查打击、信创产业化、云靶场与教育产业化、新一代智能网关产品及车联网安全等网络安全领域新兴市场开展研究和产业化工作，有利于公司进一步丰富产品结构，完善业务布局，巩固公司在网络安全领域的竞争优势。

（二）公司从事募投项目在人员、技术、市场等方面的储备情况

1、人员储备

公司一直以来注重人才引进及培养，通过完善的激励机制为员工实现自身价值提供条件，打造了一套稳定的经营团队以及与公司发展相匹配的人才结构。截至 2020 年 9 月 30 日，公司及子公司共有 2644 名员工，其中研发人员 869 名，占在职员工总数的 32.87%。经过多年积累和发展，公司形成了以核心技术人员为首的多个强有力的研发团队。公司的核心技术人员均具有丰富的行业经验与扎

实的专业知识，掌握着网络安全领域的关键技术，是公司技术水平持续提升的重要驱动力量。公司将继续坚持内部培养和外部引进相结合的人才制度，完善员工培训机制，并根据公司战略发展规划调整人力制度，提高团队素质，激发人才活力。

2、技术储备

公司自创立以来始终坚持持续技术创新的发展战略，紧跟网络信息安全技术发展趋势和用户需求，不断在行业内率先推出创新产品，更新迭代既有产品和解决方案，并孵化培育新产品。经过多年发展，公司拥有美国软件工程学会颁发的 CMMI5 权威认证，在软件开发过程的改善能力、质量管理水平、软件开发的整体成熟度居于行业前列，并掌握了应用安全与数据安全等领域的重要核心技术，形成一系列具有自主知识产权的技术成果。截至 2020 年 9 月 30 日，公司拥有超过 130 项已获授权的专利，并掌握 48 项核心技术，涉及攻防研究、应急响应、安全咨询、漏洞研究、产品研发等各个领域。

公司技术研发实力得到国家相关部门的肯定和支持，公司现已承担“国家发改委信息安全专项”、“工信部电子发展基金项目”、“科技部火炬计划”、“科技部网络空间重点专项”、“浙江省重点科技专项”等多项国家级、省市级科技计划项目，并作为主要起草单位参与多项网络信息安全领域国家及行业相关技术标准的制定，积极引领技术标准在网络信息安全产品的落地工作。

3、市场储备

公司在网络信息安全行业耕耘数十载，已成为网络信息安全领域的领先品牌，多次入选全球网络安全创新 500 强，曾先后为 2008 年北京奥运会、上海世博会、广州亚运会、连续五届世界互联网大会乌镇峰会、G20 杭州峰会、厦门金砖会议、青岛上合峰会、上海国际进口博览会、2018 第 14 届 FINA 世界游泳锦标赛等众多重大活动提供网络信息安全保障。目前，公司产品及服务已经进入了包括运营商、政府、能源、金融、教育、医疗等在内的众多行业，积累了大量优质客户，并长期保持着深入稳定的合作关系，有利于公司在满足客户信息化业务的发展规

划及建设过程的同时，动态把握客户对于信息化建设的技术需求及发展趋势，保障公司产品、解决方案及服务的竞争力。

综上所述，公司本次募集资金投资项目围绕公司现有主营业务展开，在人员、技术、市场等方面均具有良好基础。随着募集资金投资项目的建设，公司将进一步完善人员、技术、市场等方面的储备，确保募集资金投资项目的顺利实施。

五、公司应对本次发行摊薄即期回报采取的措施

本次向特定对象发行股票可能导致投资者的即期回报有所下降，公司拟通过多种措施防范即期回报被摊薄的风险，以填补股东回报，充分保护中小股东利益，实现公司的可持续发展、增强公司持续回报能力。具体措施如下：

（一）聚焦公司主营业务，提高公司持续盈利能力

本次发行的募集资金投资项目紧密围绕公司主营业务，募集资金使用计划已经管理层、董事会的详细论证，符合行业发展趋势和公司发展规划。本次募投项目的实施有利于进一步提升公司核心竞争力和可持续发展能力。

（二）加快募投项目建设，推动募投项目效益实现

公司本次发行股票募集资金的募投项目紧紧围绕公司主营业务，有利于扩大公司整体规模、扩大市场份额，增强公司资金实力，进一步提升公司核心竞争力和可持续发展能力，有利于实现并维护股东的长远利益。

本次募集资金到位后，公司将根据募集资金管理相关规定，严格管理募集资金的使用，保证募集资金按照原方案有效利用。向特定对象发行股票公司将加快推进募集资金投资项目实施，推动募投项目效益实现，从而降低本次发行对股东即期回报摊薄的风险。

（三）加强募集资金管理，提高募集资金使用效率

公司将严格按照《上市公司监管指引 2 号—上市公司募集资金管理和使用的监管要求》、《上海证券交易所科创板股票上市规则》及公司《募集资金管理制度》

的有关规定，规范募集资金使用，保证募集资金充分有效利用。公司董事会将持续监督对募集资金进行专户存储、保障募集资金用于规定的用途、配合保荐机构等对募集资金使用的检查和监督，以保证募集资金合理规范使用，防范募集资金使用风险，提高募集资金使用效率。

（四）完善公司治理，为公司发展提供制度保障

公司将严格遵循《中华人民共和国公司法》、《中华人民共和国证券法》、《上市公司治理准则》等法律、法规和规范性文件的要求，不断完善公司治理结构，确保股东能够充分行使权利，确保董事会能够按照法律、法规和公司章程的规定行使职权、做出科学、迅速和谨慎的决策，确保独立董事能够认真履行职责，维护公司整体利益，尤其是中小股东的合法权益，确保监事会能够独立有效地行使对董事、经理和其他高级管理人员及公司财务的监督权和检查权，为公司发展提供制度保障。

（五）优化公司投资回报机制，强化投资者回报机制

公司将持续根据国务院《关于进一步加强资本市场中小投资者合法权益保护工作的意见》、中国证监会《关于进一步落实上市公司现金分红有关事项的通知》和《上市公司监管指引第 3 号—上市公司现金分红》的有关要求，严格执行《公司章程》明确的现金分红政策，在公司主营业务健康发展的过程中，给予投资者持续稳定的回报。同时，公司将根据外部环境变化及自身经营活动需求，综合考虑中小股东的利益，对现有的利润分配制度及现金分红政策及时进行完善，以强化投资者回报机制，保障中小股东的利益。

公司提醒投资者，以上填补回报措施不等于对公司未来利润做出保证。投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。

六、董事、高级管理人员关于向特定对象发行股票摊薄即期回报采取填补措施的承诺

根据《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）、《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）以及中国证监会发布的《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（中国证监会公告[2015]31 号）等法律、法规和规范性文件的相关要求，为确保公司 2020 年度向特定对象发行股票摊薄即期回报采取的填补回报措施能够得到切实履行，公司董事及高级管理人员承诺如下：

“1、不无偿或以不公平条件向其他单位或者个人输送利益，也不采用其他方式损害公司利益。

2、对本人的职务消费行为进行约束，全力支持及配合公司对董事及高级管理人员职务消费行为的规范，严格遵守及执行公司该等制度及规定。

3、不动用公司资产从事与本人所履行职责无关的投资、消费活动。

4、全力支持公司董事会或薪酬与考核委员会在制定及/或修订薪酬制度时，将相关薪酬制度与公司填补回报措施的执行情况挂钩，并在公司董事会或股东大会审议该薪酬制度议案时投赞成票（如有投票/表决权）。

5、若公司后续推出或实施股权激励政策，全力支持公司将拟公布的公司股权激励的行权条件与公司填补回报措施的执行情况相挂钩，并在公司董事会或股东大会审议相关议案时投赞成票（如有投票/表决权）。

6、本承诺函出具后，若中国证监会、上海证券交易所等监管机构作出关于填补回报措施及其承诺的其他新的监管规定，且上述承诺不能满足监管机构该等规定时，本人届时将按照监管机构的最新规定出具补充承诺。

7、切实履行公司制定的有关填补回报措施以及对此作出的任何有关填补回报措施的承诺，若违反该等承诺并给公司或者投资者造成损失的，本人愿意依法承担对公司或者投资者的补偿责任。

本人若违反上述承诺或拒不履行上述承诺，本人同意按照中国证监会和上海

证券交易所等证券监管机构制定或发布的有关规定、规则，对本人作出相关处罚或采取相关监管措施。”

七、控股股东、实际控制人关于向特定对象发行股票摊薄即期回报采取的填补措施的承诺

根据《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）、《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）以及中国证监会发布的《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（中国证监会公告[2015]31 号）等法律、法规和规范性文件的相关要求，为确保公司 2020 年度向特定对象发行股票摊薄即期回报采取的填补回报措施能够得到切实履行，公司的控股股东及实际控制人范渊承诺如下：

“1、本人将严格依照相关法律、法规及公司章程的有关规定行使股东权利，继续保证上市公司的独立性，不越权干预公司经营管理活动，不侵占公司利益。

2、自本承诺函出具后，若中国证监会、上海证券交易所等证券监管机构作出关于填补回报措施及其承诺的其他新的监管规定，且上述承诺不能满足证券监管机构该等规定时，本人届时将按照证券监管机构的最新规定出具补充承诺。

3、切实履行公司制定的有关填补回报措施以及对此作出的任何有关填补回报措施的承诺，若违反该等承诺并给公司或者投资者造成损失的，本人愿意依法承担对公司或者投资者的补偿责任。

本人若违反上述承诺或拒不履行上述承诺，本人同意按照中国证监会和上海证券交易所等证券监管机构制定或发布的有关规定、规则，对本人作出相关处罚或采取相关监管措施。”

杭州安恒信息技术股份有限公司董事会

2020 年 12 月 25 日