中信建投证券股份有限公司

关于杭州迪普科技股份有限公司变更部分募集资金用途暨新增募集资金投资建设项目的核查意见

中信建投证券股份有限公司（以下简称“中信建投”、“本保荐机构”）作为杭州迪普科技股份有限公司（以下简称“迪普科技”、“公司”）2020 年度向特定对象发行股票并在创业板上市的保荐机构，根据《证券发行上市保荐业务管理办法》《上市公司监管指引第 2 号—上市公司募集资金管理和使用的监管要求》《深圳证券交易所上市公司自律监管指引第 13 号——保荐业务》《深圳证券交易所创业板股票上市规则》《深圳证券交易所上市公司自律监管指引第 2 号——创业板上市公司规范运作》等有关法律法规规定，对迪普科技变更部分募集资金用途暨新增募集资金投资建设项目事项进行审慎核查，核查情况如下：

一、变更部分募集资金用途暨新增募集资金投资建设项目概述

（一）募集资金基本情况

经中国证券监督管理委员会证监许可〔2021〕616 号《关于同意杭州迪普科技股份有限公司向特定对象发行股票注册的批复》，公司已向特定对象发行人民币普通股（A 股）29,242,293 股，募集资金人民币 1,014,999,990.03 元，扣除发行费用人民币（不含增值税）11,587,873.93 元，募集资金净额为人民币 1,003,412,116.10 元。募集资金已由立信会计师事务所（特殊普通合伙）于 2021 年 9 月 6 日审验并出具的信会师报字[2021]第 ZF10855 号《杭州迪普科技股份有限公司验资报告》确认。公司对募集资金采取了专户存储制度。

截至 2023 年 12 月 31 日，募集资金投资项目情况如下：

单位：万元

项目名称	项目总投资	承诺投入募集资金	截至期末累计投入募集资金
新一代 IT 基础设施平台研发项目	63,265.07	44,195.21	45,258.00
智能测试、验证及试制基地建设项目	67,269.25	56,146.00	190.00
合计	**130,534.32**	**100,341.21**	**45,448.00**

（二）变更部分募集资金用途暨新增募集资金投资建设项目情况

公司于近日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》，取得杭州市滨江区浦乐单元 BJ0704-M1-08 地块作为“智能测试、验证及试制基地建设项目”用地，拟将“智能测试、验证及试制基地建设项目”总投资金额由 67,269.25 万元调整为 31,392.99 万元，拟投入募集资金由 56,146.00 万元调整为 12,901.80 万元，达到预定可使用状态的日期延长至 2027 年 12 月 31 日，并将其他募集资金 43,244.20 万元投入到“下一代国产化高性能网络及安全平台研发项目”,该项目涉及的备案、环评等相关手续正在办理中。本次拟变更用途的募集资金金额为 43,244.20 万元，占公司向特定对象发行股票募集资金净额的比例为 43.10%。本次变更部分募集资金用途暨新增募集资金投资建设项目的事项不构成关联交易，不构成重大资产重组。

二、变更部分募集资金用途原因

（一）“智能测试、验证及试制基地建设项目”计划与实际投资情况

“智能测试、验证及试制基地建设项目”拟通过购进先进软硬件设备，以自建方式新建智能厂验中心、可靠性测试中心、硬件鉴定中心、新产品试制中心、智能制造中心、智能仓储中心等与公司主营业务产品相关的测试、验证、试制和仓储等场地及相关基础配套用房，实现测试、验证、试制及仓储的智能化和集中化管理，提升公司测试、验证及试制的稳定性和可靠性，提高公司经营管理能力和效率。本项目实施主体为迪普科技，实施地点为杭州高新区（滨江），拟以出让方式取得约 20,000 平方米工业用地用于项目建设。

公司于 2020 年 10 月与杭州高新开发区（滨江）经济和信息化局签署《建设项目投资意向书》，杭州高新开发区（滨江）经济和信息化局支持公司在杭州高新区（滨江）投资建设“智能测试、验证及试制基地建设项目”，并为公司提供产业项目建设用地（工业用地），面积约 30 亩，拟选址在白马湖生态创意城天马路以南、延庆寺路以西、科博特激光工程有限公司以东地块内（后续根据实际情况，经双方协商，地块位置可作调整），以市场公开挂牌方式出让。

公司持续推进“智能测试、验证及试制基地建设项目”建设，积极推动建设

用地审批程序，但由于受外部因素、地区规划等影响，取得用地进度较原计划滞后。根据杭州高新开发区（滨江）经济和信息化局 2021 年 1 月出具的《关于迪普科技“智能测试、验证及试制基地建设项目”用地的情况说明》，项目内容符合意向用地土地性质，意向用地位于允许建设区范围内，符合《杭州市土地利用总体规划（2006-2020）》；若公司无法取得意向用地，杭州市滨江区相关部门将积极协调其他可用地块供给公司。根据杭州国家高新技术产业开发区管理委员会、杭州市滨江区人民政府 2023 年 1 月公示的《2022 年重点工作目标任务整体完成情况（截至 12 月底）》，“智能测试、验证及试制基地建设项目”已经落点。根据募投项目取得用地进度，公司于 2023 年 4 月 24 日召开第二届董事会第十七次会议及第二届监事会第十四次会议，审议通过了《关于调整部分募集资金投资建设项目内部投资结构及项目延期的议案》，将“智能测试、验证及试制基地建设项目”达到预定可使用状态的日期延长至 2025 年 12 月 31 日。

根据政府统筹规划设计，结合“智能测试、验证及试制基地建设项目”项目的产业定位，经协商，杭州市滨江区相关部门协调滨江智造供给小镇可用地块供给公司，以市场公开挂牌方式出让，公司于 2024 年 2 月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》，取得杭州市滨江区浦乐单元 BJ0704-M1-08 地块（常学街以西，浦炬街以北，火炬大道绿地以东）15,397 平方米工业用地用于“智能测试、验证及试制基地建设项目”建设，并于 2024 年 3 月取得相应《不动产权证书》《建设用地规划许可证》《建设工程规划许可证》等。

截至 2023 年 12 月 31 日，“智能测试、验证及试制基地建设项目”募集资金使用情况如下：

单位：万元

项目	预计投入募集资金	累计投入募集资金	剩余募集资金（含利息）
智能测试、验证及试制基地建设项目	56,146.00	190.00	59,976.33

（二）变更“智能测试、验证及试制基地建设项目”部分募集资金用途原因

经公司董事会及管理层反复论证，根据募投项目当前实际建设情况，在项目实施主体及实施方式不发生变更的前提下，公司拟将“智能测试、验证及试制基地建设项目”总投资金额由 67,269.25 万元调整为 31,392.99 万元，拟投入募集资

金由 56,146.00 万元调整为 12,901.80 万元，达到预定可使用状态的日期延长至 2027 年 12 月 31 日，同时，将其他募集资金 43,244.20 万元投入到“下一代国产化高性能网络及安全平台研发项目”。

“智能测试、验证及试制基地建设项目”投资计划拟调整情况如下：

单位：万元

项目	投资金额	原计划投入募集资金	投资总额	调整后投入募集资金
建设工程投资	32,649.00	32,649.00	23,750.00	11,875.00
设备投资	20,812.00	20,812.00	741.80	741.80
软件投资	585.00	585.00	285.00	285.00
土地投资	2,100.00	2,100.00	1,475.00	-
预备费	2,680.30	-	1,238.84	-
铺底流动资金	8,442.95	-	3,902.35	-
合计	**67,269.25**	**56,146.00**	**31,392.99**	**12,901.80**

变更“智能测试、验证及试制基地建设项目”部分募集资金用途主要原因如下：

1、公司持续推进“智能测试、验证及试制基地建设项目”建设，积极推动建设用地审批程序，但由于受外部因素、地区规划等影响，取得用地进度较原计划滞后，取得用地面积小于原规划面积。“智能测试、验证及试制基地建设项目”原投资计划系公司于 2020 年结合当时行业发展趋势、公司实际情况等因素制定。随着公司近年来业务发展，公司产品测试、验证及试制的稳定性和可靠性提升，综合考虑公司发展战略及未来市场需求，为提高募集资金使用效率，以最少投入达成预期目标，最大限度节约募集资金，适当调减“智能测试、验证及试制基地建设项目”拟建各中心和配套用房的面积及相应的建设工程投资、设备投资、软件投资等。

2、网安市场前景广阔，公司秉持谨慎、高效使用募集资金的原则，聚焦主业，深耕安全行业，优化战略布局。随着数字中国建设推进以及云计算、大数据、物联网、AI 技术等的快速发展，安全威胁越来越复杂，网络安全的重要性持续提升，网安市场前景广阔。信创作为数字中国战略布局，是科技自主可控和国家

信息安全的基石，研发新一代基于国产芯片的大容量框式分布式架构硬件平台，并升级迭代安全防护产品、零信任安全产品、数据安全产品、应用交付产品、网络相关产品，对公司构建核心竞争力、迅速提升市场份额至关重要。依托公司在安全领域的技术积累和客户资源优势，新增募集资金投资建设“下一代国产化高性能网络及安全平台研发项目”，有利于下一代国产化高性能网络及安全平台的顺利研发及市场推广，有利于提高募集资金使用效率及维护全体股东利益。

综上，经审慎研究论证，“智能测试、验证及试制基地建设项目”对公司实现测试、验证及试制的集中化管理，提高公司经营管理能力和效率非常重要，公司将继续以自有资金和部分募集资金推进项目的建设，但基于谨慎、高效使用募集资金及维护全体股东利益的原则，结合网安市场的广阔前景，公司持续优化公司战略布局，构建信创产品核心竞争力，公司将其他募集资金投入到与主业密切相关的“下一代国产化高性能网络及安全平台研发项目”。

三、新增募集资金投资建设项目情况说明

（一）项目基本情况和投资计划

1、项目名称：下一代国产化高性能网络及安全平台研发项目

2、实施主体：杭州迪普科技股份有限公司及其全资子公司杭州迪普信息技术有限公司

3、实施地点：本项目拟在公司自有办公场地开展，不涉及土地购置事项。

4、投资计划：本项目计划总投资 62,063.40 万元，拟投入募集资金 43,244.20 万元，项目具体投资内容如下：

单位：万元

项目	投资金额	拟投入募集资金
研发费用	46,889.94	36,621.75
设备投资	6,122.45	6,122.45
软件投资	500.00	500.00
预备费	306.12	-
市场推广费用	2,602.76	-
铺底流动资金	5,642.13	-

项目	投资金额	拟投入募集资金
合计	62,063.40	43,244.20

5、建设周期：项目规划为期三年，整体进度安排如下：

实施阶段	建设期（月）											
	3	6	9	12	15	18	21	24	27	30	33	36
硬件设计、软件需求分析												
硬件测试、软件特性开发												
验证												
试产												
市场推广、产品更新												

（二）项目内容概述

本项目拟通过购进先进软硬件设备，增加研发人员投入，对安全相关产品、零信任安全相关产品、数据安全相关产品、应用交付相关产品、网络相关产品等在内的下一代国产化高性能网络及安全平台及产品进行持续研发升级和延伸。具体建设内容如下：

安全相关产品研发。基于公司现有机框式硬件平台技术积累，研发新一代基于国产芯片的大容量框式分布式架构硬件平台；基于公司原有的安全领域的积累，深化公司安全检测和技术方面的研究，从更细分具体的领域完善公司的解决方案。在公安网络领域，视频网安全联网产品符合公安视频接入要求，实现视频终端准入、签名，视频信令安全检测，视频业务转码加密、点播回放，视频终端资产管理等。动态防御安全网关产品的研发，深化公司的网关类产品的防御方案。自动化攻击规则验证平台的研发和对 AIGC 技术的研究，为自动化的攻击对抗提供新的解决思路。安全产品云地联动一体化产品及解决方案的研发，为客户提供更便利的整合方案，提升已有安全产品的竞争力。

零信任安全相关产品研发。基于零信任安全架构理念，利用安全风险持续信任评估、动态权限访问控制、权限策略自学习梳理、多场景信任度量模型构建、终端安全沙箱、终端防病毒、终端可信行为基线管控、身份统一管理与智能分析等关键技术，研发零信任安全管理平台、零信任安全代理系统、零信任安全客户端、统一身份认证平台等零信任安全产品，形成平台侧、网络侧、终端侧零信任

安全体系和解决方案。

数据安全相关产品研发。以大数据处理引擎为基础，利用数据资产识别、敏感数据识别、数据流转监控、数据脱敏、数据水印等关键技术，开发为用户提供数据安全运营能力、数据安全管控能力、数据安全监控能力的综合性数据安全治理平台。

应用交付相关产品研发。基于公司现有国产化高性能软硬件平台技术积累，深化公司在智能 DNS、集群数据和状态同步，大数据快速匹配和检索等方面的研究，研发新一代全局负载均衡产品，进一步完善公司在应用交付领域的解决方案。基于公司 200G 盒式国产化高性能软硬件平台，深化公司在 FPGA 与 CPU 配合进行应用交付业务加速、下一代 HTTP2.0 协议、DIAMETER 协议、以及 SDN 云平台、容器等对接相关技术方面的研究，进一步提升应用交付产品的核心竞争力。

网络相关产品研发。基于公司现有机框式硬件平台技术积累，研发新一代基于国产芯片的高性能、高密度、低功耗的机框式网络产品硬件平台；基于公司原有的盒式硬件平台技术积累，研发新一代基于国产芯片的高性价比的盒式交换机，提升已有网络产品的竞争力。

（三）项目可行性分析

1、项目相关背景

（1）基于国产芯片的大容量硬件平台在国内具有广阔的市场前景

在国家加速信创产业结构化的大背景下，公司积极响应政策的引导，相继推出了全系列、覆盖全部非信创款型的信创产品，现有平台最高可达到 1.2Tbps 吞吐量，该平台持续服务与金融、运营商、政府、公检法等行业，为用户的业务安全运行提供了强有力的支撑。

当前，以 5G 为代表的新一代信息技术正加速融入经济社会各领域各环节，已成为数据资源畅通循环的关键支撑，引领产业智能化、绿色化、融合化转型升级的重要引擎。在各方共同努力下，我国已建成全球规模最大、技术领先的 5G 网络。截至 2023 年 9 月末，我国累计建成开通 5G 基站 318.9 万个，5G 移动电

话用户达 7.37 亿户，5G 行业虚拟专网超 2 万个，5G 标准必要专利声明数量全球占比达 42%。5G 产业的重点将向网络质量和服务水平倾斜，下一步的产业目标将以提质、降本、增效、减碳为目标。

《中国互联网发展报告(2023)》中指出，在未来中国互联网行业将继续深入贯彻数字中国建设部署要求，进一步加强基础设施建设，千兆光网发展持续提速，稳步夯实万物互联基础；继续数据基础制度持续构建，并且不断深化数字经济和实体经济融合，加快核心技术突破，大模型技术不断快速迭代。

（2）物联网加速虚拟世界和物理世界的融合，视频网安全面临巨大挑战

经济社会数字化转型和智能升级步伐加快，物联网正在加速虚拟世界和物理世界的融合，从赋能传统产业转型升级、推动数字产业发展两个方面助力打造数字经济新优势。物联网发展迅速，其产生的数据、释放的经济价值正在快速增长。《2022-2023 中国物联网发展年度报告》中指出，当前，我国将数字经济发展提升至全新战略高度，物联网作为应用支撑技术之一，在各行业领域覆盖水平进一步提高。蜂窝物联网终端用户数量约占全球七成，物联网安全与应用国际标准研制取得新进展，智能物联网、绿色物联网等成为行业关注新方向。预计到 2023 年底全国物联网市场规模将超过 3.9 万亿元，技术融合、跨界应用等态势愈加鲜明。

中国已经建设全世界最大的视频监控联网，随之而来的视频网的安全建设尤为重要，摄像头的入侵、视频服务器的潜在威胁，其影响不仅限于隐私泄露，还正在向刑事案件乃至国防安全信息、金融交易信息、商业办公机密等领域蔓延。面对视频专网出现的种种威胁，公安部、全国各地公安机关均在研究推动视频专网安全防护建设。

（3）攻防对抗持续升级，提升企业安全产品云地联动一体化协同防护能力愈发重要

自动化攻击工具正在不断发展，未来将呈现出以下趋势：自动化程度的持续提升将减少人工干预的需要，实现攻击的更高效率。攻击工具的传播速度也将因自动化水平的提升而变得更快，这将使攻击者更难以被发现和防御。同时，攻击

工具的扫描探测流量的隐蔽性将越来越强，更难以被安全人员发现。此外，攻击工具的复杂性也将随着技术的不断发展而不断提高，使防御者更难以分析和防御攻击。

云计算的普及和发展，安全产品也开始积极利用云计算的优势。安全产品部署在云端可以提供弹性的资源分配和高效的处理能力，使其更好地适应不断变化的安全威胁。云计算还可以提供更大规模的数据存储和分析能力，使安全产品能够更好地检测和应对威胁。协同应对高级威胁是另一个重要的发展趋势。高级威胁往往更加复杂和具有针对性，传统的安全产品难以单独应对。因此，安全行业越来越重视不同安全产品之间的集成和协同工作。共享安全情报、事件响应和漏洞信息等可以提高对高级威胁的识别和应对能力。此外，跨部门和跨组织的合作也变得更加重要，以共同应对复杂的威胁。

安全行业正朝着更加智能化、协同化和综合化的方向发展。安全产品与云计算的联动、协同应对高级威胁以及对新兴技术和领域的安全需求的关注，将推动安全行业持续发展并提供更好的安全保障。

（4）全球人工智能发展逐步从“探索期”向“成长期”转变

根据行业生命周期理论（Industry Life Cycle）和 Gartner 的技术成熟度曲线模型，当前全球人工智能发展正在逐步渡过“探索期”并进入“成长期”，且已进入了全面转型的关键节点。主要有以下四个关键特征：

①人工智能专用技术迅速突破

专用人工智能即面向特定领域的人工智能（即“弱人工智能”），由于其具备任务单一、需求明确、应用边界清晰、传统领域知识丰富和功能建模相对简单等特征，因此在重点领域形成技术突破后，随即进入了快速的商业化应用阶段，成为人工智能迈向“成长期”的底层支撑。目前，人工智能主要的应用技术方向包括以深度学习为代表的机器学习算法；以计算机视觉、图像识别、语音识别为代表的智能感知技术；以及以无人驾驶、自动机器人等为代表的自主无人系统的三大领域。

②人工智能产业生态蔚然成型

从全球范围内看，围绕专用人工智能技术的人工智能产业已经初具规模。据德勤（Deloitte）预测，2025 年世界人工智能总体市场规模将超过 6 万亿美元，2017—2025 年复合增长率达 30%。在产业链上，形成了包括智能芯片、传感器、智能设备厂商的硬件层；数据分析处理、算法模型、软件开发和关键技术厂商的技术层；行业应用、解决方案、产品服务开发厂商的应用层等三大层级体系，整体产业生态发展开始从“探索期”的弥补市场空白向“成长期”的产业结构优化转型发展。

③人工智能投融资日趋理性成熟

创投研究机构 CB Insights 发布的《全球人工智能投资趋势年度报告》显示，AI 初创公司超过 70%的投融资为早期投资或 A 轮融资，资金向头部初创企业集中的趋势明显加强。伴随着“探索期”的风险投资甚至跟风投机泡沫的消除，核心技术、商业落地和可持续发展成为投资者最关切的决策因素，投融资整体趋向理性必然带来产业结构的优化，驱动人工智能从“探索期”向“成长期”发展。

④人工智能应用场景向深层拓展

目前，人工智能的应用场景包括金融、零售、医疗、教育、政务、制造、汽车、家居、智慧城市、数字内容、公共安全等多个垂直领域。相关行业场景的应用深度不一。中国新一代人工智能发展战略研究院对 797 家中国人工智能骨干企业中的 581 家应用层企业进行了详细分析，提供企业技术集成与方案提供、智能机器人两个应用领域的人工智能企业数占比最高，分别为 15.43%和 9.66%。紧随其后的是关键技术研发和应用平台、新媒体和数字内容、智能医疗、智能硬件、金融科技、智能商业和零售、智能制造领域。可以说，“探索期”的人工智能发展将主要向更多应用领域过渡，“成长期”的人工智能应用将向更深层次渗透。

（5）全球零信任技术与体系兴起，进入快速发展阶段

2010 年，Forrester 分析师约翰.金德维格(John Kindervag)首次提出了零信任安全的概念，即“所有的网络流量都是不可信的，需要对访问任何资源的任何请求进行安全控制”。该理念颠覆了传统边界安全架构思想，是应对新 IT 时代网络安全挑战的全新战略，因此其理念一经提出便引起了网络安全产业界的关注。谷

歌率先孵化出了以零信任为基础的“BeyondCorp”项目，旨在让员工在不受信任的网络中无需接入 VPN 就能顺利工作。BeyondCorp 项目构建了中心化的认证、授权和访问控制系统，真正且彻底地改变了企业的安全体系，是全球第一个零信任理念的落地实践，至此零信任概念得到了网络安全产业界更为广泛的认可。

零信任已经从一个新兴安全理念发展成为全球网络安全的关键技术，商业模式走向成熟，市场逐步规模化，已成为了政企数字化转型的首选安全战略。以美国为首的发达国家高度重视零信任能力建设。自 2019 年起，美国陆续发布零信任指导建议、计划等推动零信任在美落地，其他发达国家也纷纷在零信任领域展开布局，以强化网络空间话语权。2022 年 11 月 22 日，美国国防部发布了《国防部零信任战略》和《国防部零信任能力执行路线图》，计划在 2027 年之前实施战略和相关路线图中概述的独特的零信任能力和活动。2023 年 4 月 11 日，CISA(美国网络安全和基础设施安全局)发布第二版零信任成熟度模型，旨在降低美国机构实施零信任的壁垒。种种举措显示美国正加速在零信任领域的研究与应用。

我国已从多层级启动零信任标准研究，协助建立产业规范。为落实国家网络信息安全相关要求，我国已从多层级开展零信任标准研究国际标准方面，由中国企业主导的 ITU-T(国际电信联盟电信标准分局)零信任国际标准《服务访问过程持续保护指南》正式发布；国家标准方面，全国信息安全标准化技术委员会正在开展《信息安全技术 零信任参考体系架构》的编制：行业标准方面，中国通信标准化协会正在开展《面向云计算的零信任体系 第 2 部分：关键能力要求》、《面向云计算的零信任体系 第 6 部分：数字身份安全能力要求》、《面向云计算的零信任成熟度评价模型》、《零信任安全技术参考框架》与《网络安全产品能力评价体系 第 11 部分：基于零信任架构的业务安全平台评价方法》等标准的研究工作。

（6）数据安全政策升级，急需催熟 5G 场景数据安全技术

面对日益严峻的数据安全威胁，全球发达经济体包括美国、欧盟、英国等纷纷把数据竞争力上升为国家战略高度，更加重视数据竞争力，纷纷制定出台数据战略，宣誓数据安全和主权；在保护数据安全的前提下，承认数据价值、促进数据利用，力争在数据政策及标准制订等方面建立领导力。2019 年 12 月，美国发布《联邦数据战略和 2020 年行动计划》，以 2020 年为起始点，规划了美国政府

未来十年的数据愿景，核心思想是将数据作为战略资源来开发,通过确立一致的数据基础设施和标准实践来逐步建立强大的数据治理能力，为美国国家经济和安全提供保障。

我国也相继出台了诸多法律法规和监管标准。2019 年 7 月，在 G20 大阪峰会的数字经济特别会议上，中国提出“共同完善数据治理规则，确保数据的安全有序利用；要促进数字经济和实体经济融合发展，加强数字基础设施建设，促进互联互通；要提升数字经济包容性，弥合数字鸿沟”，“数据安全”上升到我国国家安全战略高度。2021 年 9 月，《中华人民共和国数据安全法》颁布实施，标志着国家对个人信息和政务信息重视程度进一步提高。2021 年 8 月，《中华人民共和国个人信息保护法》颁布实施，统合私主体和公权力机关的义务与责任，兼顾个人信息保护与利用，奠定了我国网络社会和数字经济的法律之基。

国内 5G 数据安全领域处于起步探索阶段，急需突破关键技术、提高数据安全产品成熟度，促进 5G 数据安全产业长足发展，保障 5G 场景下数据安全。

（7）国家持续推动数字经济建设，加大信息基础设施建设

“十四五”规划纲要提出，围绕强化数字转型、智能升级、融合创新支撑，布局建设信息基础设施、融合基础设施、创新基础设施等新型基础设施。扩容骨干网互联节点，新设一批国际通信出入口，全面推进互联网协议第六版（IPv6）商用部署。实施中西部地区中小城市基础网络完善工程。推动物联网全面发展，打造支持固移融合、宽窄结合的物联接入能力。加快构建全国一体化大数据中心体系，强化算力统筹智能调度，建设若干国家枢纽节点和大数据中心集群，建设 E 级和 10E 级超级计算中心。

2022 年 2 月，国家发改委、中央网信办、工业和信息化部、国家能源局联合印发通知，同意在京津冀、长三角、粤港澳大湾区、成渝地区启动建设国家算力枢纽节点，此前，内蒙古、贵州、甘肃、宁夏 4 地算力枢纽节点已获批复。至此，全国一体化大数据中心体系完成 8 大国家算力枢纽节点，10 个国家数据中心集群的总体布局设计，“东数西算”工程正式全面启动。这也将直接拉动数据中心基础设施相关产业链。

国家数字化转型的深入推进，大数据、区块链、高性能计算、边缘计算、人工智能等信息技术快速发展，智能制造、智慧金融、车联网、卫星互联网等“高算力、大连接、强安全”的应用场景不断涌现，带来持续攀升的算力和网络需求。算网融合聚焦“计算”+“网络”协同发展，整合异构计算、网络、存储等多种资源进行统一调度和智能编排，构建融合、智能、安全的新型服务模式，对于产业来说意义重大。算网融合不仅能够驱动新一轮的内生性经济增长，为宏观经济形势注入投资新动能，还可以助力关键技术实现突破，培育产业发展链条，赋能地方经济实现全面转型。

2、项目实施的必要性

（1）研发新一代大容量框式分布式架构硬件平台，满足国产高端领域产业网络安全需求

本项目旨在以国产芯片为基础，研发新一代大容量框式分布式架构硬件平台，公司将在芯片认证引入、电路板设计、整机结构优化、加工制造、软件合作、产品试制试验等多方面形成产业化布局，带动上下游生产合作企业进一步提升国产化能力与水平，为行业内高端市场国产化产品产业化及规模应用积累经验。本平台，将加强顶层设计，推动技术融合，加大核心技术攻关力度，以应用场景创新为牵引，促进 5G 核心网、大数据、云计算等技术的融合创新，提升 5G 融合应用供给能力，为 5G 在生产生活中更广泛、更深入地应用提供助力，同时以为客户降本增效为主要目标，推动产品在绿色节能方向继续保持行业领先水平。

随着骨干网的加速建设，以及网络业务流量的高速增长，现有基于国产芯片的网络安全产品也急需同步更新换代，在产品性能、可靠性、绿色节能等方面满足新增需求。研发一款满足未来 5 年行业使用需求，未来 3 年内行业领先的新一代基于国产芯片的大容量框式分布式硬件平台，将为公司未来的国产高端领域产业布局产生至关重要的作用。

（2）面对物联网、视频网安全新威胁，急需安全联网专用设备

随着我国城市化进程的发展，视频监控系统作为维护社会公共安全的重要载体和工具，遍布城市各个角落和人民日常生活的各个领域，其功能和作用愈发显

著。公安视频传输网的建设规模正在不断扩大，专网前端的 IP 接入设备的种类与数量正在不断上升（存量超过 1 亿个），这些前端设备被广泛应用于治安管理、交通疏导、智慧小区管理等领域，与国计民生息息相关；同时，如人脸对比、车辆识别、大数据分析等核心业务，也正向公安视频传输网迁移，目前的公安视频传输网事实上已经成为一张承载海量终端与海量数据的物联网。

公安视频传输网的重要性正在不断提升，随之而来的安全问题也日益凸显，一旦出现黑客攻击、数据窃取等事件，将有可能造成治安管理失控、交通管制失效、敏感信息泄漏、LED 屏幕导流信息被篡改等后果，严重危害社会稳定。因此，如何解决来自于前端设备的安全风险、如何防护视频传输网的安全、如何监测视频传输网中的异常情况成为公安视频传输网安全体系建设的重要问题。

视频物联网安全已经上升到国家安全层面，国家相继推出了多个国标、行标（公安），如 GB/T21741-2021 及 GA/T1781-2021 等标准，旨在解决当前视频专网的的网络安全威胁。

（3）利用 Web 动态防御技术，逐渐成为应对 Web 安全挑战新手段

当前超过 75%的网络攻击目标是针对企业的 Web 服务，其中 90%以上是自动化攻击。传统 Web 防御产品通常采用基于规则的检测方法，对流量进行被动检测和处置，这种方式容易被攻击者绕过，无法及时发现新型攻击和零日漏洞的利用，导致安全性无法得到有效保障。此外，传统 Web 防御产品需要处理大量的流量，对设备的性能和处理能力提出了很高的要求，高性能低延迟的处理要求增加了产品开发、部署和维护的成本，限制了产品的可扩展性和灵活性。

Web 动态防御技术优势：1）采用更加先进的安全防护技术和策略，如反向代理安全加解密防御安全代理，通过对解密流量进行改写和安全业务处置，能够有效应对各类攻击和威胁，提升 Web 应用的安全防护能力。2）专注于研究移动目标防御技术，抵御来自机器人、自动化工具和 0Day 利用工具的攻击。通过不断分析和研究最新的攻击方式和威胁情报，及时更新和优化防护策略，提高对新型攻击和威胁的防御能力。3）采用 Web 页面的指纹生成和客户端指纹采集技术，通过多种数据综合判定客户端类型，有助于准确区分正常用户和恶意攻击者，提高对恶意行为的识别和拦截能力，有效降低误报率和漏报率。4）针对高性能低

延迟的处理要求进行优化，提高产品的性能和响应能力。通过采用新技术架构设计，实现高效的流量处理和并发连接管理，提高产品的可扩展性和灵活性，满足不同时间的大规模流量处理需求。5）采用自动化的安全防护机制，通过机器学习和智能算法实现实时的攻击检测和防护，减轻维护人员的工作负担，降低维护成本和压力。

基于以上 Web 动态防御技术优势，急需 Web 动态防御产品，在成本可控的情况下，提升企业 Web 安全能力。

（4）基于多种检测防护技术与服务的安全产品云地联动一体化解决方案成重要趋势

传统防御方式的主旨是将攻击者拒之门外，然而随着攻击手段的多样化、隐蔽化、复杂化，传统的防御方式往往疲于应付，企业需要一种技术手段，主动对抗攻击行为，采取有利于防守方的技术措施，对攻击者形成震慑，保护数据安全。

Orca Security 最近的一份报告分析了网络犯罪习惯。该报告显示，攻击者通常会在短短两分钟内找到暴露的“秘密”，允许访问企业云环境的敏感信息片段，并且在许多情况下，几乎立即开始利用它们。该研究于 2023 年 1 月至 2023 年 5 月进行，首先是在九种不同的云环境中创建“蜜罐”，模拟云中配置错误的资源以吸引攻击者。每个都包含一个秘密的 Amazon Web Service(AWS)密钥。云端蜜罐技术可以帮助企业诱捕攻击者、收集攻击信息、分析攻击行为，降低奇特部署和维护成本的同时，提升企业的安全防护能力，发现并响应安全威胁。

此外，IDC 发布了《IDC Technology Assessement:中国公有云托管安全服务能力，2023》报告，核心覆盖专家能力、生态建设、漏洞及威胁检测、事件分析、威胁情报、远程事件响应、威胁狩猎七个维度，中国公有云托管安全服务未来的技术发展趋势加快。面对网络攻击，全球数字化转型成功的企业除了部署专业的安全产品外，仍然需要安全产品及服务提供商提供专业的安全服务，帮助客户有效利用安全产品、设定安全策略、分析攻击行为，并及时处置形成闭环管理。

进入数字时代，网络攻防对抗正在向纵深发展，网络攻击方将目光从核心服务器、业务系统、数据库逐渐转向国家关键基础设施，如石油化工、电网、交通、

水利以及一些工业自动化领域，都已经成为网络攻击的重灾区。在实网攻防的深刻变革下，传统的单点式、链式、被动式防御已无法应对高级威胁，数字时代更需体系化作战。通过基于多种检测防护技术与服务的安全产品云地联动，目的就是采用“云上云下一体化”模式，将云端与本地资源进行深度融合，实现企业内外部安全防护的无缝对接，打造出统一、高效的联动产品和解决方案。

（5）我国零信任市场规模高速增长，零信任产品及解决方案应用前景广阔

IDC 正式发布《IDC MarketShare：中国零信任网络访问解决方案市场份额，2022：共筑信任城墙》、《IDC MarketShare：中国零信任网络访问场景之软件定义边界市场份额，2022：核心应用场景的规模化引领市场稳步发展》和《IDC MarketShare：中国零信任网络访问场景之终端安全市场份额，2022：终端场景应用成为市场发展新动能》三份报告，上述三份报告对 2022 年中国零信任网络访问解决方案以及其核心应用场景市场的规模、增长速度、主要玩家、市场与技术的发展趋势等内容进行了详细研究。

2022 年，中国零信任网络访问解决方案市场规模约为 2.67 亿美元（约 17.9 亿元人民币），规模同比增长 30%。在威胁形势、业务需求等因素的推动下，全球零信任网络访问市场开始快速发展。根据 IDC 预测数据显示，全球零信任网络访问（ZTNA）解决方案的市场规模将在未来几年保持快速增长，2022 至 2026 年的年复合增长率将达到 30.3%，预计 2023 年市场规模将增长至 22 亿元，中国零信任网络访问解决方案市场也将跟随全球趋势保持高速增长态势不断发展。

“下一代国产化高性能网络及安全平台研发项目”中对零信任安全相关产品的研究，有利于公司加强对零信任安全技术的布局，解决行业用户场景下的安全问题，有利于公司满足日益增长的零信任安全需求。

（6）我国 5G 技术发展提速，数据安全保护供给不足，产业解决方案需求强烈

近年来，我国数字经济蓬勃发展成为国家竞争力的重要体现。作为引领新一代信息技术和新型基础设施的核心，5G 技术在数字经济发展中扮演着重要的角色。在中央和地方政府的持续推动以及产业界的积极参与下，中国的 5G 发展进

入了快车道。然而，随着 5G 的高速发展，对于 5G 数据安全的需求日益突出。特别是企业客户在引入 5G 网络后，面临着敏感数据被窃取、泄露、丢失或滥用等风险的担忧。由于通信模式的改变，企业网络增加了新的边界，并带来了边缘计算所带来的新的云安全问题。在 5G 网络建设已进入高速发展的背景下，企业用户迫切需要具备专业的 5G 安全能力和服务。加大对 5G 垂直领域数据安全产品的投入，有助于公司巩固其核心技术领先优势，保持竞争力，并在行业中取得长足的发展。

然后，数据安全相关产业对于 5G 数据安全保护供给不足。一方面，我国 5G 网络仍处于发展导入期，当前产业发展政策主要以网络建设、生态示范为重点，我国各省市区出台的 5G 政策文件包括发展规划、行动计划、实施方案、基站规划建设支持政策等，主要致力于推进 5G 网络建设、应用示范和产业发展，缺少 5G 数据安全层面关注。另一方面，国内数据安全技术产业发展方兴未艾，数据安全产品、解决方案、服务体系尚未成熟，存在数据安全保障基础薄弱、数据安全产品类型与解决方案单一等问题，针对 5G 应用的数据安全技术产品防护水平有待提升。

公司覆盖运营商、政府、金融、公安、交通、企业、科教文卫等行业，产品和解决方案在运营商市场得到了广泛的认可和应用，并在三点运营商集采中连年名列前茅，占据行业领先地位。本项目将扩大公司在 5G 数据安全垂直领域的技术领先性，使公司具有完善 5G 场景化数据安全产品和解决方案，抓住 5G 快速发展所带来的巨大商机，增强核心竞争力，扩大在行业的领先优势，提升赢利能力。

（7）数字经济时代，新型数字基础设施成为源动力

数字经济要求数字基础设施具备高速稳定的网络连接能力。数字经济的核心在于数据的传输和处理，因此一个快速稳定的网络是不可或缺的。数字基础设施需要有足够的带宽和低延迟，以满足数字经济中大数据、云计算、人工智能等应用的需求。同时，数字经济还要求数字基础设施提高可靠和高可用，以确保用户能够随时随地访问和使用数字经济的服务和应用。

到 2025 年末，我国 IPv6 网络规模、用户规模、流量规模将位居世界第一。

全面支持网络、应用、终端的 IPv6 升级，并成功实现向下一代互联网的平滑演进。这将使我国在全球范围内领先，形成一个具备高度竞争力的下一代互联网技术产业体系。

DNS 作为 IPv6 网络演进的基础，是推动下一代互联网产业体系基础设施升级的基石，是提升互联网业务可靠性和访问质量的关键技术，是支撑互联网业务蓬勃发展的核心产品之一。同时应用交付产品也是作为确保互联网业务能够快速、安全、可靠地访问，有效改善用户体验的重要手段之一。

应用交付产品作为网络与应用系统之间的桥梁，已经被广泛应用于金融、电信、教育、医疗、政府、商业创新等领域的核心业务系统前以及出口链路场景，在业务流量爆发式增长的大背景下，应用交付设备在网络中的地位越发凸显。

3、项目实施的可行性

（1）信息安全行业规模持续扩张，市场细分领域产业结构不断完善

IDC 数据显示，2022 年全球网络安全 IT 总投资规模为 1890.1 亿美元，并有望在 2027 年增至 3288.8 亿美元，五年复合增长率（CAGR）为 11.7%。随着网络安全“三法一条例”的稳步推进和实施，IDC 预测，中国网络安全市场规模从 2022 年的 123.5 亿美元快速增长至 2027 年的 233.2 亿美元，期间年复合增长率为 13.5%，高于全球平均水平。未来中国网络安全市场将更加成熟，在整体技术市场组成中，安全防御硬件设备逐步云化，网络安全软件和服务市场持续增长，五年复合增长率分别为 16.7%和 16.3%。

5G 关键技术创新突破取得新进展，灵活高效的 5G 网络将带来更快、更密集的数据流，传统的通过加密、访问控制、隔离等技术手段保护存储系统的“保险柜”模式已无法满足数据流动安全防护的需求，数据安全保护重点将由原来静态的数据存储系统防护转变为动态的数据流动全生命周期风险管控，需要进一步构建以数据为中心的治理方案。

我国加大政策保障，推动零信任落地。目前我国正在从政策、行业实践、产业发展等多个层面对零信任进行积极探索，工业和信息化部通过多种举措引导零信任发展，前期以推动零信任理论研究和技术创新为主，后期加强零信任技术应

用，推动项目落地。《网络安全产业高质量发展三年行动计划(2021-2023 年)》发布，重点围绕“加快开展基于开发安全运营、主动免疫、零信任等框架，推动创新技术发展与网络安全体系研发。加快发展动态边界防护技术，鼓励企业深化微隔离、软件定义边界、安全访问服务边缘框架等技术产品应用”等内容展开。多个零信任项目入选重点领域试点示范项目名单，包括“2022 年网络安全技术应用试点示节项目名单”“2021 年大数据产业发展试点示范项目名单”等。

各类互联网业务的快速发展，网络承载了金融、医疗、生产办公、交通调度、生活消费等各行各业的关键业务，各类业务应用的可靠性和访问质量变得日益重要，因此用户对应用交付产品的需求变得日益强烈。同时，在应用交付行业，国外厂商起步较早，前期一直处于垄断地位。近年来，虽然国内厂商在应用交付市场的份额正在逐步增加，但是相关产品尤其是在 200G 以上高性能产品的 CPU、内存等核心器件仍然采用国外产品，国产化应用交付市场保持着快速增长，市场空间广阔。

（2）公司重视研发投入，坚持技术创新，具备扎实的人才储备及技术积累

信息安全行业属于知识密集型行业，技术、知识的更新换代迅速，自成立以来，公司在网络安全产品、应用交付产品及基础网络产品等 IT 基础设施领域持续进行研发投入，坚持技术创新，建立了扎实的人才储备和技术积累。

在人才储备方面，公司具有一支业界领先的研发队伍，并通过一系列有效的聘用、培训和激励机制保障团队稳定。截至 2023 年末，公司在北京和杭州设有研发中心，一共拥有研发员工 608 名，占公司员工总数的 35.98%，其中核心技术团队在 IT 基础设施领域拥有丰富的研发、管理经验，尤其是在高性能硬件架构、FPGA 系统设计、大型软件平台技术、信息安全和应用交付领域核心算法、安全研究和安全服务相关技术等方面具有深厚积累。公司拥有专业的安全攻防实验室、一流的安全研究团队以及各类业界高等级的安全服务资质，相关研究成果能够迅速转化为产品能力，为持续提升公司安全产品的防护能力、确保公司在市场竞争中保持技术领先性提供了有力保障。

在技术积累方面，自成立以来，公司以“让网络更简单、智能、安全”为愿景，持续进行研发创新，并自主开发了基于多核 CPU、FPGA 芯片以及分布式转

发技术的高性能硬件平台“APP-X”，全面融合网络、安全、应用交付功能的 L2~7 融合操作系统“ConPlat”，将应用特征库、攻击特征库以及病毒库三库合一的应用识别与威胁特征库“APP-ID”。在此基础上，依托于安全研究团队十多年以来在攻防研究、漏洞挖掘、威胁情报分析、安全事件响应等技术积累，公司开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模、AI 特征分析的异常行为检测、基于上下文语义分析的敏感数据识别、数据动态脱敏等技术，并连续两年获得“中国人工智能大赛”最高等级 A 级证书。公司形成了一系列具有自主知识产权的核心技术。截至 2023 年末，公司已授权发明专利 1,435 项，技术成果转化成为实际生产力方面有足够的储备和能力，公司以这些核心技术为基础，推出了涉及网络安全、应用交付、基础网络等 IT 基础设施主要应用领域的共十几大类上百款产品，形成了有较强竞争力的完备产品线。围绕“让网络更简单、智能、安全”的核心目标，公司在相关产品和解决方案上已经形成鲜明技术特点和领先技术优势，同时，通过完备的产品布局和系统的安全服务能力，可以为用户提供完善的整网解决方案，真正实现“交钥匙”工程。

公司在网络安全产品、应用交付产品及基础网络产品等 IT 基础设备领域的人才储备和技术积累将有助于项目得到更好地实施。

（3）公司深耕信息安全行业，具备良好的客户资源、品牌口碑和营销服务体系

自成立以来，基于对网络信息安全发展趋势及用户需求的深刻理解，公司以“让网络更简单、智能、安全”为愿景，一直专注于企业级网络通信产品的研发、生产、销售以及为用户提供相关专业服务，形成了良好的客户资源、品牌口碑和营销服务体系。

在客户资源方面，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、电力能源、金融、教育、医疗、交通等在内的众多行业，积累了大量客户，并长期保持着深入稳定的合作关系，这些客户自身具有雄厚的实力并在业界拥有良好的信誉，极大降低了公司的经营风险和财务风险。公司通过在上述行业的长期耕耘与积累，与行业内的大量客户达成了紧密合作，积累信息化

建设及信息安全建设项目的实施经验，完善产品功能，满足客户信息化业务的发展规划及建设思路，动态把握主要领域客户对于信息化建设的技术需求及发展趋势，可以进一步提高公司产品、解决方案及服务的竞争力。此外，公司已经在各大行业建立了数量众多的样板点，可以对更大范围的用户起到较好的辐射和示范效应，为公司实现持续快速发展、进一步扩大领先优势打下了坚实基础。

在品牌口碑方面，公司产品和服务的用户已经遍及全国各个省份以及众多行业，通过优质的产品质量、领先的解决方案以及专业的服务，公司在客户中树立了良好的企业形象，并且建立起了良好口碑和品牌。作为国内信息安全产业的重要厂商之一，公司是“国家信息安全漏洞库一级技术支撑单位”、“信息安全标准化技术委员会成员单位”、“中国网络安全产业联盟常务理事单位”。同时，公司还获得了“国家知识产权示范企业”、“国家重点软件企业”、“国家高新技术企业”等多项荣誉。广大用户、行业同仁以及国家相关部门对公司的认可，体现出公司在信息安全行业的品牌已得到广泛认可。

在营销服务体系方面，公司在全国设有 27 个办事处，通过持续的市场拓展，公司已建立起覆盖全国的市场销售与技术支援体系，公司对行业价值客户的信息化建设和网络安全需求的理解和把握能力，使公司针对价值客户所提供的产品及服务赢得了广泛认同。公司拥有专业的安全服务与研究团队，能够自行挖掘安全漏洞，提供安全评估、安全应急等服务；具有本地化服务能力，能保证对用户突发事件的及时响应。公司广泛发展渠道合作伙伴，现拥有 2,500 余家认证代理商，公司已经建立了覆盖众多细分行业市场的完备的营销和服务渠道体系。目前，公司的办事处、售后服务机构与渠道合作伙伴之间形成了良好的互动，使得公司的产品和服务能得到快速推广。

（4）公司法人治理结构完善，内控体系健全

公司已按照上市公司的治理标准建立了以法人治理结构为核心的现代企业制度，健全了各项规章制度和内控制度，并在日常经营过程中不断地改进和完善，形成了较为规范的公司治理体系和完善的内部控制环境。在募集资金管理方面，公司制定了《募集资金管理制度》，对募集资金的存储、使用进行了明确规定。健全的治理体系、内控制度和募集资金管理制度，能够促进募投项目的顺利实施，

保证募集资金合理规范使用。

4、项目实施面临的风险及应对措施

本项目是在公司原有技术基础上的进一步开发和升级，拟研发的各类产品均系以公司现有产品为基础实现功能的提升和应用场景的延伸，公司在相关项目中对诸多关键技术难点进行了预研和攻关，有效降低了项目整体风险。但技术的升级开发具有不确定性，如未能按期完成研发计划，可能会导致新产品推出时间延后、新技术开发进度不达预期、研发遭遇技术瓶颈甚至失败，将对公司进一步提升产品竞争力带来不利影响。

公司将时刻关注行业发展方向，预测技术发展趋势，以国家政策为指导，以市场为导向，基于长期行业实践积累的经验不断调整研发创新及相应产品转化以降低项目实施风险。

（四）项目经济效益分析

本项目是对公司现有产品进行的升级研发，研发升级后的产品实现的效益是公司对相关产品历史累计投入的结果，无法单独核算因本次募集资金使用而产生的效益。根据公司现有竞争优势、技术积累以及行业发展趋势，预期本项目实施后，将对公司收入、利润产生积极影响。

四、变更部分募集资金用途暨新增募集资金投资建设项目的影响

本次募投项目调整是公司基于谨慎、高效使用募集资金及维护全体股东利益的原则，经充分审慎研究论证，公司募集资金投入的新项目属于主营业务，前景广阔，符合国家产业政策和公司整体战略发展方向，有利于优化公司战略布局，构建信创产品核心竞争力，提高募集资金的使用效率，为公司和股东创造更大效益。符合《上市公司监管指引第 2 号——上市公司募集资金管理和使用的监管要求》《深圳证券交易所创业板股票上市规则》《深圳证券交易所上市公司自律监管指引第 2 号——创业板上市公司规范运作》等相关法律、法规的规定。公司将严格遵守有关募集资金使用的相关规定，加强募集资金使用的内部与外部监督，确保募集资金使用合法、有效。

五、决策程序情况

公司于 2024 年 4 月 15 日召开第三届董事会第六次会议与第三届监事会第六次会议，审议通过了《关于变更部分募集资金用途暨新增募集资金投资建设项目的议案》，同意公司变更“智能测试、验证及试制基地建设项目”部分募集资金用途暨新增募集资金投资建设“下一代国产化高性能网络及安全平台研发项目”。

六、保荐机构核查意见

经核查，本保荐机构认为：

公司变更部分募集资金用途暨新增募集资金投资建设项目事项，已经第三届董事会第六次会议与第三届监事会第六次审议通过，尚需提交 2023 年度股东大会审议。公司本次变更部分募集资金用途暨新增募集资金投资建设项目是公司根据市场环境变化及公司业务发展需要等因素作出的审慎决策，有利于提高募集资金使用效率，不存在损害公司和中小股东合法利益的情形，符合《上市公司监管指引第 2 号——上市公司募集资金管理和使用的监管要求》《深圳证券交易所创业板股票上市规则》《深圳证券交易所上市公司自律监管指引第 2 号——创业板上市公司规范运作》等相关规定。

本保荐机构对公司变更部分募集资金用途暨新增募集资金投资建设项目事项无异议，该事项尚需公司股东大会审议通过后方可实施。

（以下无正文）

（本页无正文，为《中信建投证券股份有限公司关于杭州迪普科技股份有限公司变更部分募集资金用途暨新增募集资金投资建设项目的核查意见》之签章页）

保荐代表人签字：

吴继平　　赵润璋

中信建投证券股份有限公司

2024 年 4 月 15 日