证券代码：002439　　证券简称：启明星辰　　公告编号：2019-089

债券代码：128061　　债券简称：启明转债

启明星辰信息技术集团股份有限公司

关于部分变更募集资金用途的公告

本公司及董事会全体成员保证信息披露内容的真实、准确和完整，没有虚假记载、误导性陈述或重大遗漏。

启明星辰信息技术集团股份有限公司（以下简称“公司”）于 2019 年 12 月 9 日召开第四届董事会第七次会议，审议通过了《关于部分变更募集资金用途的议案》，该议案尚须提请公司可转换公司债券持有人会议及股东大会审议，现将有关情况公告如下：

一、基本情况概述

（一）公司公开发行可转换公司债券募集资金基本情况

经中国证券监督管理委员会《关于核准启明星辰信息技术集团股份有限公司公开发行可转换公司债券的批复》（证监许可[2018]2159 号）核准，公司于 2019 年 3 月公开发行可转换公司债券，每张面值为人民币 100.00 元，募集资金款以人民币缴足，共计人民币 104,500.00 万元，扣除发行费用 11,692,924.53 元，募集资金净额为人民币 1,033,307,075.47 元。上述资金于 2019 年 4 月 2 日到位，已经瑞华会计师事务所（特殊普通合伙）验证并出具瑞华验字[2019]44050002 号验证报告。

公司已根据相关规定将上述募集资金进行了专户存储管理，并与存放募集资金的银行签署了募集资金三方监管协议。截至 2019 年 10 月 31 日止，本公司有 7 个募集资金专户，募集资金存放情况如下：

单位：元

开户银行	银行账号	募集资金余额
招商银行北京分行上地支行	531905618810402	1,843,042.22
杭州浣纱支行	33106618001880002 3689	-
北京银行股份有限公司友谊支行	20000040512800028336592	1,954,140.95
北京银行股份有限公司友谊支行	20000040514100028338197	-
中国民生银行股份有限公司北京分行	688002224	-

中国民生银行股份有限公司北京分行	662022229	-
中国光大银行股份有限公司北京德胜门支行	35010188000148324	825,200,371.90
合 计		828,997,555.07

注：募集资金余额包括银行存款利息扣除银行手续费之净额。

（二）变更部分募集资金投资用途的概述

为提高募集资金使用效率，根据公司发展规划及募投项目实际情况，公司拟对公司公开发行可转换公司债券的部分募集资金投资项目做出变更，具体拟减少对募集资金投资项目“郑州安全运营中心和网络安全培训中心建设项目”投入的募集资金，并部分变更募投项目实施地点，即新增募集资金投资项目“重庆安全运营中心建设项目”和“天津安全运营中心建设项目”。

公司第四届董事会第七次会议、第四届监事会第六次会议审议通过了《关于部分变更募集资金用途的议案》。公司独立董事对上述事项发表了独立意见。根据《公司章程》《公司募集资金管理制度》等相关规定，该议案尚需提交公司可转换公司债券持有人会议及股东大会审议。变更前后募集资金投资项目的情况如下表：

变更前			变更后		
序号	项目名称	计划投入募集资金（万元）	序号	项目名称	计划投入募集资金（万元）
1	郑州安全运营中心和网络安全培训中心建设项目	33,000.00	1	郑州安全运营中心和网络安全培训中心建设项目	15,700.00
			2	重庆安全运营中心建设项目	14,825.63
			3	天津安全运营中心建设项目	2,474.37

二、变更募集资金投资项目的情况说明

（一）原募投项目计划和实际投资情况

原募集资金投资项目“郑州安全运营中心和网络安全培训中心建设项目”拟在河南省郑州市高新技术产业集聚区投资建设，项目投资总额为 50,500 万元，其中：建设投资拟使用募集资金 33,000 万元，用于资本性支出的购置办公场所、装修、研发设备购买。拟使用自筹资金用于非资本性支出的研发费用 10,000 万元、铺底资金 3,000 万元。项目建设期为 3 年，项目通过购买办公楼、配置先进

的硬件设备和软件工具，整合公司生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力；从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

截至 2019 年 10 月 31 日，该项目已累计投入金额 0.00 元，募集资金余额（含募集资金存放期间产生的利息）均存放于募集资金专户。

（二）变更原募投项目的原因

自 2018 年以来，特别是《信息安全技术网络安全等级保护基本要求》发布后，政策推动网络安全产业发展进入了快车道。同时网络安全面临的威胁日趋严重，安全运营中心已成为技术创新和服务创新的重要抓手。

建设城市安全运营中心是公司既定发展战略，在积极筹备推进可转债募投项目建设的同时，公司使用自有资金在全国范围内大力推进安全运营中心建设，先后通过自建及合作方式在山东青岛、青海西宁、贵州贵阳、四川成都、四川攀枝花、湖北宜昌、河南三门峡、河南漯河、广东广州（南沙）、浙江德清等省会城市、地级城市建设安全运营中心。通过广泛实践，发现在国内政策的大力推动、安全威胁的日趋严峻的形势下，用户对安全运营中心的业务需求和创新需求日渐迫切，且呈现出新的发展特点：从中东部重点区域向全国各省发展、从省会级城市向地级市发展、从服务商引导需求建设向用户主动要求建设发展、从服务商自建场地设备才能投入运营向部分有条件的用户主动提供场地和部分设备发展。同时，由于用户需求的蓬勃发展，越来越多的网络安全厂商开始进入城市安全运营中心市场。公司具有先发优势，且安全运营中心业务具有独特的用户粘性，因此迅速拓展市场显得尤为重要。

鉴于重庆、天津等地安全运营中心的建设迫在眉睫，急需迅速完成建设投入以满足当地政府机关、企事业单位对于网络安全防护的需求。同时基于 2017 年市场的发展态势，郑州安全运营中心和网络安全培训中心建设项目原计划投资 50,500 万元，希望通过郑州市安全运营中心的建设辐射服务全省。目前公司已在积极筹备募投项目建设，在当地租赁房产开展前期的网络安全服务。因两年来政

策快速推进，安全运营中心从省会城市正在向地级市发展，部分有条件的用户也能够提供建设场地和部分设备。通过强有力的业务运作，现河南省内除郑州市外，公司在三门峡和漯河市的安全运营中心已依次落地，其他省内地级城市正在积极拓展中，从而使得原在省会城市建设安全运营中心服务全省的模式正在演进到效率更高的省会城市与地级城市并举建设的模式，也一定程度上能够节约省会城市的项目投资、提高资金使用效率、更快地占领市场，因此计划减少对郑州安全运营中心和网络安全培训中心建设项目投资金额。

公司综合考虑外部政策环境对市场的推动作用、用户解决安全问题的迫切需求、自身在城市安全运营中心建设的实践和保持竞争中的领先地位的战略需要，以及公司对安全服务市场演进趋势的判断等因素，拟变更部分募集资金的用途。公司计划将部分“郑州安全运营中心和网络安全培训中心建设项目”的部分募集资金投入到“重庆安全运营中心建设项目”、“天津安全运营中心建设项目”，进一步强化公司在重庆、天津等地的业务布局，提高服务当地客户的能力，从而能够满足对各区域城市各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力，为上市公司安全服务业务带来更多优质客户和订单，有助于提高募集资金的使用效率，提升公司的盈利能力，推动上市公司更好更快的发展，从而为股东创造更多价值。

三、新募投项目情况说明

(一) 郑州安全运营中心和网络安全培训中心建设项目基本情况和投资计划

1、新募投项目名称：郑州安全运营中心和网络安全培训中心建设项目

2、项目实施主体：郑州启明星辰信息安全技术有限公司及其全资子公司郑州市启明星辰企业管理有限公司

3、项目建设地点：郑州市郑州高新技术产业集聚区雪兰路与枫香街交汇处

4、项目建设性质：新建

5、项目建设内容：本项目计划建设启明星辰郑州安全运营中心和网络安全培训中心，致力于公司河南省信息安全运营业务及综合解决方案的研发和市场拓展，并成立网络安全培训中心，为我国培养网络安全人才。

6、项目建设期：3 年。

7、项目投资计划

投资总额为 21,000 万元，拟使用募集资金 15,700 万元，用于资本性支出的购置办公场所、装修、研发设备购买，不包含非资本性支出的研发费用 2,800 万元、铺底资金 2,500 万元（含铺底流动资金 1,715 万元、涨价预备费 785 万元），非资本性支出自筹资金解决。具体资金运用情况见下表：

郑州安全运营中心和网络安全培训中心建设项目投资估算表

单位：万元

	购置办公场所	装修	设备	研发费用	铺底资金	合计
投资额	10,000	2,500	3,200	2,800	2,500	21,000
占总投资的比例	47.62%	11.90%	15.24%	13.33%	11.90%	100%

8、项目经济效益分析

本项目全部达产后预计年均销售收入为 15,766.65 万元，年均净利润 6,030.74 万元，扣除所得税后内部收益率 21.96%，静态投资回收期（税后，含建设期）为 6.20 年。

9、本项目已取得郑州高新技术开发区管理委员会经济发展局出具的《河南省企业投资项目备案证明》，项目代码：2019-410172-65-03-067183。

(二) 重庆安全运营中心建设项目基本情况和投资计划

1、新募投项目名称：重庆安全运营中心建设项目

2、项目实施主体：重庆启明星辰信息安全技术有限公司和其全资子公司启明星辰（重庆）企业管理有限公司

3、项目建设地点：重庆市渝北区财富大道 1 号

4、项目建设性质：新建

5、项目建设内容：本项目计划建设公司重庆安全运营中心，致力于进行重庆地区安全运营业务及其综合解决方案的研发及市场拓展。

6、项目建设期：2.5 年。

7、项目投资计划

投资总额为 19,325.63 万元，拟使用募集资金 14,825.63 万元，用于资本性支出的购置办公场所、装修、研发设备购买，不包含非资本性支出的研发费用

2,500.00 万元、铺底资金 2,000.00 万元（含铺底流动资金 1,661.39 万元、涨价预备费 338.61 万元），非资本性支出自筹资金解决。具体资金运用情况见下表：

重庆安全运营中心建设项目投资估算表

单位：万元

	购置办公场所	装修	设备	研发费用	铺底资金	合计
投资额	10,553.44	1,272.19	3,000.00	2,500.00	2,000.00	19,325.63
占总投资的比例	54.61%	6.58%	15.52%	12.94%	10.35%	100%

8、项目经济效益分析

本项目全部达产后预计年均销售收入为 15,234.61 万元，年均净利润 5,790.69 万元，扣除所得税后内部收益率为 24.59%，静态投资回收期（税后，含建设期）为 5.51 年。

9、本项目已取得重庆市渝中区发展和改革委员会出具的《重庆市企业投资项目备案证》，项目代码：2019-500103-65-03-101335。

(三) 天津安全运营中心建设项目基本情况和投资计划

1、新募投项目名称：天津安全运营中心建设项目

2、项目实施主体：天津启明星辰信息技术有限公司

3、项目建设地点：天津自贸试验区（中心商务区）宝晨大厦 22 层 2202 号

4、项目建设性质：新建

5、项目建设内容：本项目计划建设公司天津安全运营中心，致力于进行天津地区安全运营业务及其综合解决方案的研发及市场拓展。

6、项目建设期：2.5 年。

7、项目投资计划

投资总额为 5,657.71 万元，拟使用募集资金 2,474.37 万元，用于资本性支出的研发设备购买，不包含非资本性支出的租赁办公场所 183.34 万元、研发费用 2,000 万元、铺底资金 1,000 万元（含铺底流动资金 776.28 万元、涨价预备费 223.72 万元），非资本性支出自筹资金解决。具体资金运用情况见下表：

天津安全运营中心项目投资估算表

单位：万元

	租赁办公场所	装修	设备	研发费用	铺底资金	合计
投资额	183.34	-	2,474.37	2,000.00	1,000.00	5,657.71

占总投资的比例	3.24%	-	43.73%	35.35%	17.67%	100%

8、项目经济效益分析

本项目全部达产后预计年均销售收入为 9,361.98 万元，年均净利润 3,551.04 万元，扣除所得税后内部收益率为 74.40%，静态投资回收期（税后，含建设期）为 3.43 年。

9、本项目已取得天津高新技术开发区管理委员会经济发展局出具的《天津市企业投资项目备案证明》，项目代码：2019-120316-64-03-463143。

（四）项目的可行性分析及项目面临的风险及控制措施

1、项目宏观背景

（1）网络信息安全市场在全球范围内快速发展

近年来，全球网络威胁持续增长，网络罪犯在恶意代码和服务的开发、传播和使用上愈发趋于专业化，目的愈发趋于商业化，行为愈发组织化，手段愈发多样化，造成的损失也随着范围的扩散而快速增多，2018 年全球知名企业都遭遇了重大泄漏事件，欧盟在 2018 年出台了一般数据保护条例，对个人信息的保护和监管达到了前所未有的高度，其他国家和地区也正在讨论和制定类似的数据保护条例。

严峻的网络安全态势驱动着全球信息安全市场快速增长，根据赛迪顾问发布的《2019 中国网络安全发展白皮书》，2018 年全球网络信息安全市场规模达到 1269.8 亿美元，同比增长 8.5%，未来几年随着 5G、物联网、人工智能等技术的全面普及，网络安全市场规模将继续保持稳定上涨，至 2021 年整个行业规模有望达到 1648.9 亿美元。

（2）网络空间安全上升到国家战略高度为行业的发展营造了良好的契机

近年来，各类敌对势力、利益团伙网络空间攻击能力在不断提升，国家级组织间网络冲突日益增多，当前在网络空间中面临的安全挑战日益复杂。信息安全已经牵涉到国家安全问题。2016 年 4 月 19 日，习近平主席在主持召开中央网络安全和信息化领导小组第一次会议时强调，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。他还指出，没有网络安全就没有国家安全，没有信息化就没有现代化。2016 年 12 月 27 日，

国家互联网信息办公室发布了《国家网络空间安全战略》，阐明了中国关于网络空间发展和安全的重大立场和主张，明确了包含捍卫网络空间主权、维护国家安全、保护关键信息基础设施等在内的主要任务。网络安全作为顶层设计列入国家的战略规划中，使得行业得到极大的催化。

承接国家网络空间安全战略，《“十三五”国家信息化规划》提出了“强化网络安全顶层设计”、“构建关键信息基础设施安全保障体系”、“全天候全方位感知网络安全态势”、“强化网络安全科技创新能力”四大战略任务，从法律体系、技术能力等各个层面，全方位绘制出加强网络安全保障能力的内容和方法。可以预见，有顶层设计为指导、基础设施保障体系为基础、态势感知能力为手段、创新能力为核心竞争力，必将推动中国网络安全保障能力更上一层楼。

（3）中国网络安全政策密集发布，为行业发展提供了保障

中国关于网络安全的政策不断出台，多项加强网络安全技术研发、推进产业发展和网络安全人才培养的法律法规和政策措施密集发布，为网络安全产业的发展提供了良好的政策保障。

2016 年，国家通过了新《网络安全法》，从法律层面明确提出国家实行网络安全等级保护制度，指出网络运营者应当按照网络安全等级保护制度的要求，制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；2017 年 7 月 11 日，国家互联网信息办公室发出《关键信息基础设施安全保护条例（征求意见稿）》明确规定，地市级以上人民政府应当将关键信息基础设施安全保护工作纳入地区经济社会发展总体规划，加大投入，开展工作绩效考核评价。国家对关键信息基础设施的重点关注催生出对网络安全服务的需求。

随着大数据、云计算等网络新技术快速发展，网络空间受到的威胁越来越复杂，影响越来越恶劣，给网络安全工作带来巨大的挑战，备受国家关注。2017 年 3 月 30 日，国家电子政务外网管理中心办公室组织发布了《政务云安全要求》，该标准对云计算国家标准在电子政务应用方面的安全要求做了补充，为指导全国各级政务部门开展政务云服务提供安全和管理依据，保证政务云服务的安全要求。2017 年 4 月，全国信息安全标准化技术委员会发布了《大数据安全标准化白皮书》，重点介绍了国内外的大数据安全法规政策、标准化现状，重点分析了

大数据安全面临的安全风险和挑战，给出了大数据安全标准化体系框架，规划了大数据安全标准工作重点，提出了开展大数据安全标准化工作的建议；

近几年，网络安全领域重要制度建设明显加快，2019 年 5 月以来《网络安全审查办法》《数据安全管理办法》《儿童个人信息网络保护规定》《网络关键设备安全检测实施办法》《个人信息出境安全评估办法》《网络安全漏洞管理规定》等重要制度相继完成向社会公开征求一件，进入修改完善阶段。2019 年 7 月国家网信办、国家发展改革委、工业和信息化部、财政部联合发布《云计算服务安全评估办法》对党政机关、关键信息基础设施运营者采购使用云计算服务提出更高的安全要求。

国家在网络安全人才培养方面也出台了相应的支持政策。《网络安全法》从法律层面提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，采取多种方式培养网络安全人才，促进网络安全人才交流。2017 年 8 月 14 日，国家网信办在官网发布《一流网络安全学院建设示范项目管理办法》，提出在 2017 年至 2027 年实施一流网络安全学院建设示范项目，建成 4 至 6 所“国内公认、国际上具有影响力和知名度”的网络安全学院的目标。多项支持政策为企业开办网络安全培训中心提供了契机，也为校企合作、企企合作创造了条件。

（4）云计算、大数据、移动互联等技术的发展拓宽安全防护领域，为行业带来了挑战和机遇

由国家安全战略角度延伸到区域城市级安全环境来看，以智慧城市为核心承载体，大数据、物联网、移动互联、云计算普及的社会环境下，网络相关设备智能化、规模化、小型化、多样化的特点越发明显，伴生了网络空间复杂、网络环境多变、网络风险增高等安全方面的各种问题，成为影响社会经济健康发展的重要制约因素。

国家计算机网络应急技术处理协调中心发布的《2016 年中国互联网网络安全报告》中描述到：

- 高级持续性威胁常态化，中国面临的攻击威胁尤为严重；
- 针对工业控制系统的攻击日益增多，多起重要工业控制系统安全事件应引起重视；

- 大量联网智能设备遭受恶意程序攻击形成僵尸网络，被用于发起大流量 DDoS

攻击；

- 网站数据和个人信息泄漏屡见不鲜，衍生灾害严重；
- 移动互联网恶意程序趋利性更加明显，移动互联网黑色产业链已经成熟；
- 敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全。

总的来看，新技术环境下网络安全的要求更多、更高，传统的网络安全产品和服务难以满足市场需求，对于整个网络安全行业来说，既是一项挑战也是一次机遇。

（5）政府在智慧城市建设中网络安全意识显著提升

在“互联网+”时代背景下的智慧城市建设高度集成了物联网、云计算、大数据等众多新形态的信息技术，这些都是实现城市职能智能化的基础，是一项复杂的大型系统工程，从传感感知层、通信传输层、应用层、智能分析处理等诸多层面存在安全风险和脆弱性，具有区别于传统网络时代特点的信息安全风险。一旦在网络安全防护上不能得到有效保证，可能造成城市管理职能出现混乱、隐私信息泄露、应急决策失误、各类事故频发乃至局部社会动荡的局面。

近几年，随着智慧城市的高速发展，与智慧城市相关的网络安全事件频发，长期维持在较高水平，引起了国家高度关注。2014 年 8 月，八部委联合发布的智慧城市建设的纲领性文件《关于促进智慧城市健康发展的指导意见》中明确了要完善管理机制，“要加快研究制定智慧城市建设的标准体系”。2015 年 11 月国家标准委联合中央网信办及国家发展改革委印发《关于开展智慧城市标准体系和评价指标体系建设及应用实施的指导意见》(国标委工二联〔2015〕64 号，以下简称《意见》)。《意见》明确到 2017 年，将完成智慧城市总体、支撑技术与平台、基础设施、建设与宜居、管理与服务、产业与经济、安全与保障 7 个大类 20 项急需标准的制订工作，到 2020 年累计完成 50 项左右的标准。

2、项目微观背景

（1）中国网络信息安全市场处于快速成长期，安全服务市场态势向好

①中国网络信息安全市场概况

与全球网络信息安全市场相比，中国信息安全行业正处于快速成长期，信息

安全需求从核心业务安全监控向全面业务安全保护扩展，从网络实施阶段的安全布置到网络运行过程的安全维护，安全需求正在向更高层次、更广范围延伸，安全服务的市场需求不断扩大。

②中国网络信息安全市场规模

2018 年，网络安全政策法规持续完善，网络安全市场规范性逐步提升，政企客户在网络安全产品和服务上的投入稳步增加，2018 年国内网络信息安全市场整体规模达到 495.2 亿元，随着数字经济发展、5G，以及物联网建设的逐步推进，网络安全作为数字经济发展的必要保障，其投入将持续增加，根据赛迪顾问提供的数据显示，预测到 2021 年网络安全市场规模将达到 926.8 亿，增长率均保持在 20%以上。

③网络信息安全服务市场态势向好

网络信息安全产品包括三部分：硬件、软件和服务。在全球市场中，随着云安全和移动安全等新型领域安全的发展，安全服务化理念深入人心，安全服务和安全软件成为发展热点，2018 年安全服务和安全软件的市场份额分别为 807.6 亿美元、332.7 亿美元，占比 64%和 26%。

目前中国网络信息安全市场仍是以硬件为主。虽然信息安全硬件市场占比最大，但是市场规模增长率持续下跌，由 2017 年的 49.6%下降到 2021 年的 41.3%。相反，服务市场表现出持续上升的势头，从 2017 年的 12.8%上升到 2021 年的 19.8%，增速高于信息安全产品市场，中国网络信息安全服务市场态势向好。

随着中国信息产业和网络技术的发展，传统的网络信息安全产品难以满足日益变化的复杂的网络空间，中国的信息安全产品行业必将向国际看齐，由硬件为主转换为服务为主。目前国内信息安全领域的重要企业，如 360、绿盟、卫士通、天融信等，均在开展行业解决方案策划和推广工作，从产品导向型企业向服务导向型企业转变，以适应未来用户定制化服务和细分市场等发展趋势。

④网络安全服务模式转型大步推进，正向网络安全运维模式过渡

由于网络安全行业的产品众多，大到集团公司小到部门，都可能需要针对单个产品进行单独招标，并且为了防止一家独大，往往出现刻意分散招标的情况，导致网络安全行业出现小公司林立、市场集中度较为分散的格局，而由于分散招标，很难形成各种网安产品的立体联动防御和大数据分析，网络安全公司也很难

提供有效的整体安全服务。但是随着大数据、云模式以及需求升级的三级推动，网络安全行业有望从当前的产品采购模式逐步向安全运维模式过渡，并且高壁垒决定了行业竞争格局走向集中。

（2）网络安全培训市场人才供应严重不足，专业安全分析人才缺乏

①网络安全培训市场概况

网络安全是以“人”为核心的，究其原因，网络安全领域的对抗本质上是人与人之间的对抗，而网络终端、网络设备以及各种工具仅仅是作为辅助手段而存在的，但是，网络安全人才培养速度远跟不上快速发展的网络安全市场，市场缺口达到90%以上，因此如何创新的培养高素质的网络安全人员，让其学好网络安全的理论、掌握网络安全技能、提高网络安全对抗水平，是亟需解决的问题。

②中国网络安全人才供应严重不足

根据智联招聘发布的2017年的《网络安全人才市场状况研究报告》的数据显示，2017年上半年，通过智联招聘发布的网络安全岗位招聘需求，较2016年上半年同比增长了232%。但根据教育部2015年发表的《中国教育概况》的数据显示，2015年，全国共有普通、成人高等学校2852所，但开设《信息安全》相关专业的院校仅有64所，占比仅为全国高等学校总数的2.2%。网络安全专业的学生培养滞后于市场的需求。

随着互联网技术的应用进一步普及，加上《网络安全法》、国家网络安全等级保护制度的强力推动下，国内广大政企机构将会迅速形成对网络安全人才的紧迫需求。东南大学网络空间安全学院常务副院长程光在接受澎湃新闻采访时称，根据我国医生、护士对应全国总人口的比例来计算，我国网络安全人才缺口是70万；而以我国警民比例作为参考的话，计算出的结果大概在70-140万之间。

截至2020年，中国网络安全人才需求量将达到160万人，每年网络安全专业毕业生人数仅为1万人，巨大的需求缺口需要通过专业的安全人才培训机构填补。如果不能够增加人才供给量，未来网络安全人才缺口将越来越大。

③网络安全市场专业安全分析人才匮乏

目前，安全行业内人才培养偏重两类。第一类是大专院校培养的科班出身的安全人才，偏重于各类安全理论知识，缺乏应用经验；第二类是各类攻防演练平台培养的安全人才，偏重于攻击渗透，但缺乏安全事件分析、防御方面的体系化

能力。专业的安全分析师十分稀缺，且集中在专业的网络安全公司，一些政府机构和其他领域企业难以获得这方面的人才。

3、项目建设可行性分析

（1）该项目具有良好的市场前景

网络信息安全市场行业痛点多，市场潜力巨大。由于各行业对网络系统的依赖越来越强，攻击造成的业务停止服务的危害、以及公民个人信息为代表的数据泄露、损毁所造成的影响越来越大，甚至在某些情况下，安全事件会直接导致公民生命安全受到威胁；但是深入的分析，现有的安全解决方案还是基于传统的产品部署模式和服务模式，不足以面对不断升级的网络安全攻击行为。

2017 年 5 月，当我们应对 WannaCry 勒索病毒的威胁时所采用的方法，与十余年前应对冲击波、震荡波蠕虫病毒时的手段并未有本质的区别，还是依靠断网、单机查杀病毒去处理，从造成这种现象的原因分析看，主要在以下几个方面：

- 在网络运营者一侧的问题：

各类机构在网络建设的过程中采购了大量安全产品，但是缺乏专业使用人员，导致无法确认安全产品是否在正常发挥作用；安全产品的无效部署带来虚假的安全感，可能会因为问题处理不及时，反而造成的损失会更高。

- 在安全设备厂商一侧的问题：

安全厂商在新技术领域不断研究推出新型产品，如最近结合威胁情报、大数据分析推出的相关态势感知类、高级威胁防御类产品，但是此类产品对于前端使用人员的要求不是降低，而是更高；产品距离用户需求非但没有拉近，而是更远。

- 传统网络安全服务的局限：

传统的安全服务是安全评估、渗透测试、安全咨询类服务，此类服务都是基于年度或单次的安全服务，只能在某个阶段对某一特定系统的安全状态进行评价，无法持续的进行监测以应对持续的来自内外部的威胁。

所以，郑州安全运营中心、重庆安全运营中心、天津安全运营中心可以利用云计算、大数据等先进技术为当地的客户提供高效的网络安全运营和维护服务，可以有效缓解政府、企业网络安全运营人员短缺和能力不足的问题，通过集中、持续的网络安全监测，提高政府、企业面对网络安全突发事件的应急能力，减少损失，从而有效缓解长期困扰客户网络安全运营的难题。网络安全培训中心的成

立能够解决专业化的人才供不应求的问题。

（2）国家相关政策的大力支持

近几年，国家出台了大量的法律、法规，旨在推动网络安全市场的健康有序发展，为安全运营中心的建立，提供了法律支持。网络信息安全相关政策如下表：

时间	发文单位	名称	主要内容
2019 年 7 月	工业和信息化部	《加强工业互联网安全工作的指导意见》	要求加快构建工业互联网安全保障体系，形成覆盖工业互联网生命周期的事前防范、事中监测和事后应急能力
2018 年 12 月	工业和信息化部	《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
2016 年	全国人大常委会	《网络安全法》	进一步界定关键信息基础设施范围；对攻击、破坏我国关键信息基础设施的境外组织和个人规定相应的惩治措施；增加惩治网络诈骗等新型网络违法犯罪活动的规定等
2015 年	工信部	《国务院关于积极推进“互联网+”行动的指导意见》	加快安全可靠服务器、存储系统、桌面计算机及外部设备、网络设备、智能终端等终端产品、基础软件和信息系统的研发与推广
2014 年	工信部	《加强电信和互联网行业网络安全工作的指导意见》	对网络基础设施和业务系统安全防护、推进安全可控关键软硬件应用、网络数据和用户个人信息保护等做出强调。
2014 年	中央军委	《关于进一步加强军队信息安全工作的意见》	加强信息安全工作是适应信息时代发展的必然要求，是实现能打仗打胜仗核心要求的紧迫任务，必须把信息安全工作作为军事斗争准备的保底工程，采取超常、务实举措解决突出矛盾和重难点问题，促进我军信息化建设科学发展、安全发展。
2014 年	银监会	《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》	从 2015 年起，各银行业金融机构对安全可控信息技术的应用以不低于 15%的比例逐年增加，并要求安排不低于 5%的年度信息化预算，到 2019 年安全可控信息技术在银行业总体达到 75%左右的使用率。

资料来源：整理于公开资料

（3）公司是国内信息安全领域的领军企业

①产品线充裕完备，多领域位居首位

公司成立于 1996 年，是国内少数拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。

在产品方面，公司拥有完善的专业安全产品线，横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域，共有百余个产品型号，并根据客户需求不断增加。其中统一威胁管理（UTM）、入侵检测与防御（IDS/IPS）、安全管理平台（SOC）均取得市场占有率第一的成绩（长江证券研究），同时在安全性审计、安全专业服务方面保持市场领先地位，其它还包括防火墙（FW）、Web 应用防火墙、漏洞扫描、互联网行为管控、终端安全、数据防泄密、无线安全引擎、应用交付、网闸、数据安全交换、大数据处理/安全、电子印章/签名、工控安全等多个产品类型。随着云计算时代的到来，公司已完成大部分产品的虚拟化、云化工作，并推出满足政务云/行业云、大数据应用、智慧城市、态势感知、移动互联安全等新需求的新产品与解决方案。

②公司在行业中具有技术服务优势

公司拥有代表国内最高水准的技术团队，包括积极防御实验室（ADLab）、网络安全博士后工作站、研发中心、安全运营中心、安全咨询专家团（VF 专家团）、安全系统集成团队等，构成了公司重要的核心竞争力。公司在系统漏洞挖掘与分析、恶意代码检测与对抗等上百项安全产品、管理与服务技术方面拥有完全自主知识产权的核心技术积累。此外，公司还是国家认定的企业级技术中心、国家规划布局内重点软件企业，拥有最高级别的涉及国家秘密的计算机信息系统集成资质，并获得国家火炬计划软件产业优秀企业、中国电子政务 IT100 强等荣誉。公司拥有我国规模最大的国家级网络安全研究基地，创造了百余项专利和软件著作权，参与制订国家及行业网络安全标准，填补了我国信息安全科研领域的多项空白。完成包括国家发改委产业化示范工程、国家科技部 863 计划、国家科技支撑计划、核高基重大专项等国家级科研项目上百项。

（4）公司的良好盈利能力为战略性扩张打下基础

自成立以来，公司销售业绩已连续多年保持高速增长。年度财务审计报告显示，截止到 2018 年 12 月 31 日，公司及其权益核算的合资公司总资产 49 亿元（合并报表口径）。近三年来，总资产保持持续的增长态势。

2018 年，公司实现营业总收入 25.22 亿元，归属于上市公司股东净利润 5.69

亿元。近五年来，营业收入保持持续增长，利润也呈增长趋势，公司财务状况良好。

显而易见，公司的良好盈利能力为战略性扩展打下基础。

（5）公司在网络安全培训方面具有丰富的经验

1996 年，启明星辰集团培训认证部成立，2017 年公司网络空间安全学院正式成立，是国内最早的安全培训机构之一，作为国内权威的网络安全培训机构，在培训的技术先进性、广度与深度，以及培训服务体系的质量和规模方面都深受行业推崇。

网络空间安全学院先后承担过国家各部委、教育、电信、金融、能源等行业的安全培训工作，正逐步形成安全运维课程体系、安全攻防课程体系、安全管理课程体系、安全技术课程体系、新技术安全课程体系、认证类课程体系、软件安全开发类课程体系、源代码安全审计课程体系等八大课程体系近 60 门课程。到目前为止，公司网络空间安全学院已为各行业客户培养了累计达 30,000 多名安全技术和管理人员，组织安全竞赛集训 40 次，培训安全竞赛获奖人员近 500 名，被国内外合作伙伴誉为“中国极具实力的高质量培训机构”。

①具有多项国内外信息安全方面培训资质

经过多年的发展和实践，公司培训部获得了国内外多项培训资质。

- CISP——国家信息安全测评中心；
- CISSP——ISC²官方授权培训服务商（国际注册信息系统安全专家）；
- NSACE——工业和信息化部教育与考试中心；
- 通信网络安全服务能力评定 – 安全培训一级资质；
- 通信网络安全知识技能竞赛“优秀支撑单位”。

②具有专家型的师资队伍

公司公司内部拥有 17 名专业的覆盖全面的网络安全培训师，多人通过了国内外培训讲师认证，并且有 2 人获得“金圆丁”奖。

③具有系统的课程体系

依托公司在安全领域拥有的核心技术，并依据多年来对客户的培训服务，结合不同行业的特点，公司网络空间安全学院创立了一套卓有成效的培训体系，包含国际国内安全认证培训、安全攻防竞赛培训、安全知识及前沿技术培训三大板

块，分层次分角度兼顾安全知识的各个方面，为客户提供定制化培训方案。

4、项目实施风险及应对措施

（1）技术风险风险及应对措施

信息安全技术正处于不断变化的阶段，只有掌握最新技术发展动向，才能及时应对攻击和管理问题。因此对于本项目安全运营中心的建设速度和应变能力要求相当高。且安全运营中心要针对各种大型企业，实施服务复杂，有的还需要定制，对信息安全公司的研发及服务能力均提出了很高要求。

公司依据自身二十余年来在网络安全领域的技术经验积累，能保证自身核心技术的有效实施。同时，公司拥有国内一流的研发队伍，有专门的实验室、研究院，以及一批专业人员，包括：黑客攻防技术研究团队——积极防御实验室（ADLab），安全运营服务团队——M2S 安全运营中心，安全体系设计及咨询团队——VF 前线技术专家团，安全系统集成团队和国内首家企业网络安全博士后工作站。他们一直保持跟踪各类安全技术动态发展，因此能够有效化解技术风险，在核心技术不断跟进的措施上将会领先一步。

（2）管理风险及应对措施

中国 IT 行业人才流动频繁，很多资金雄厚的互联网企业不惜重金获得有技术、有经验的软件开发人才，给国内小规模企业带来了项目脱节、技术泄密等各方面损失。如何建立科学的管理制度，提高内部管理水平，最大限度释放员工的创造力，并有效保护企业自身的知识产权及技术机密将成为信息安全企业面临的重要课题。

软件产业的核心就是人才，而对于安全公司人员队伍的稳定同样是关键，其中有能力、经验的研发人员又是重中之重。公司将充分发扬民族企业团队精神，同时加强资本市场运作，保证高水平人才的待遇，并为其提供更加广阔的发展空间。通过合理配置人力资源，全面激活员工个体的责任意识和行为能力。

公司将致力于将研发、生产、销售融为一体，促使研发者摆脱实验性研发的心态，使其所采取的技术路线与管理者提出的商业途径相吻合，即开发策略与公司运行策略相匹配，所研发的产品必须具有自主知识产权，能够与国际标准接轨。

（3）市场程序风险及应对措施

国内网络信息安全市场发展非常迅速，市场份额也在不断增大，虽然项目前景非常广阔，但是项目面临激烈的市场竞争，尤其国内同类厂商纷纷进入该领域，未来的几年的竞争将会更加激烈。

针对重点行业和规模化市场，进一步巩固和拓展公司在山东区域的营销渠道和客户群体，持续市场渗透，不断扩大市场占有率，拓宽市场覆盖面，细化行业运营管理，使安全运营服务更加贴近重点行业客户需求，做到真正解决用户痛点。

（4）政策程序风险及应对措施

国内信息安全行业受国家政策影响，为了保护信息安全，国家出台了很多限制性政策，比如，等级保护制度，重点保护关键信息基础设施、明确规定网络运营者的责任。所以，现在安全服务必须满足政策的要求，在当地建立安全服务运营中心，但是，随着互联网、大数据、云计算、物联网技术的进步，国家的政策也会随之调整，未来的发展也许会因为政策的调整而改变。

随着互联网、大数据、云计算、物联网技术的进步，监管部门在信息安全方面的政策法规也许会改变，对数据安全保护政策也会放宽，所以，必须做好两手准备，应对政策的变化。

四、独立董事、监事会、保荐机构对本次变更事项的意见

（一）独立董事意见

经审核，公司关于部分变更可转换公司债券募集资金用途的事项，是结合公司发展情况作出的调整，符合公司的实际生产经营情况，内容及程序符合《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》《深圳证券交易所中小企业板上市公司规范运作指引（2015 年修订）》等相关规定，有利于更加合理、有效地使用募集资金。公司本次变更部分可转换公司债券募集资金用途，未改变募集资金投资项目的使用方向，仍为公司主营业务，不存在变相改变募集资金投向的损害股东利益的情况。本次变更履行了规定的程序，符合维护公司发展利益的需要。独立董事同意公司此次变更部分可转换公司债券募集资金用途的事项，并同意将该议案提交公司可转换公司债券持有人会议及股东大会审议。

（二）监事会核查意见

经审核，监事会认为，公司本次部分变更可转换公司债券募集资金用途的事项与公司主营业务发展方向一致，新项目的实施能够扩大公司主要产品生产能力，进一步提升公司主要产品市场地位，符合公司发展战略方向。有利于提高募集资金的使用效率，符合全体股东利益。相关审议程序符合法律规定，本次变更部分可转换公司债券募集资金用途的事项有利于公司整体发展，不存在损害股东利益的情形，符合现行有关上市公司募集资金使用的相关规定。监事会同意公司本次变更部分可转换公司债券募集资金用途的事项。

（三）保荐机构对本次变更事项的意见

经核查，保荐机构认为：公司根据战略发展要求，对募集资金投资项目进行部分变更，有利于公司提高募集资金使用效率，符合公司和全体股东利益，不存在损害公司和中小股东利益的情形。公司已经履行了必要的审批程序，以上事项尚需提交公司可转换公司债券持有人会议及股东大会审议。

综上，保荐机构对本次变更事项无异议。

五、备查文件

1、启明星辰第四届董事会第七次会议决议；

2、启明星辰第四届监事会第六次会议决议；

3、独立董事关于第四届董事会第七次会议相关事项的独立意见；

4、光大证券股份有限公司关于公司变更部分募集资金用途的核查意见。

特此公告。

启明星辰信息技术集团股份有限公司董事会

2019 年 12 月 10 日