中信建投证券股份有限公司关于
奇安信科技集团股份有限公司
2021 年半年度持续督导跟踪报告

2020 年 7 月 22 日，奇安信科技集团股份有限公司（以下简称“公司”、“奇安信”）在上海证券交易所科创板上市。根据《科创板首次公开发行股票注册管理办法（试行）》、《证券发行上市保荐业务管理办法》及《上海证券交易所科创板股票上市规则》等相关规定，中信建投证券股份有限公司（以下简称“中信建投证券”、“保荐机构”）为首次公开发行股票并在科创板上市的保荐机构，对奇安信进行持续督导，持续督导期为 2020 年 7 月 22 日至 2023 年 12 月 31 日。

2021 年半年度，中信建投证券对奇安信的持续督导工作情况总结如下：

一、持续督导工作情况

序号	工作内容	持续督导情况
1	建立健全并有效执行持续督导工作制度，并针对具体的持续督导工作制定相应的工作计划	保荐机构已建立健全并有效执行了持续督导制度，并制定了相应的工作计划
2	根据中国证监会相关规定，在持续督导工作开始前，与上市公司签署持续督导协议，明确双方在持续督导期间的权利义务，并报上海证券交易所备案	保荐机构已与奇安信签订《持续督导协议》，该协议明确了双方在持续督导期间的权利和义务
3	持续督导期间，按照有关规定对上市公司违法违规事项公开发表声明的，应于披露前向上海证券交易所报告，并经上海证券交易所审核后在指定媒体上公告	2021 年半年度，奇安信在持续督导期间未发生按有关规定须保荐机构公开发表声明的违法违规情况
4	持续督导期间，上市公司或相关当事人出现违法违规、违背承诺等事项的，应自发现或应当自发现之日起五个工作日内向上海证券交易所报告，报告内容包括上市公司或相关当事人出现违法违规、违背承诺等事项的具体情况，保荐人采取的督导措施等	2021 年半年度，奇安信在持续督导期间未发生违法违规或违背承诺等事项
5	通过日常沟通、定期回访、现场检查、尽职调查等方式开展持续督导工作	保荐机构通过日常沟通、定期或不定期回访、现场检查等方式，了解奇安信经营情况，对奇安信开展持续督导

		工作
6	督导上市公司及其董事、监事、高级管理人员遵守法律、法规、部门规章和上海证券交易所发布的业务规则及其他规范性文件，并切实履行其所做的各项承诺	在持续督导期间，保荐机构督导奇安信及其董事、监事、高级管理人员遵守法律、法规、部门规章和上海证券交易所发布的业务规则及其他规范性文件，切实履行其所做出的各项承诺
7	督导上市公司建立健全并有效执行公司治理制度，包括但不限于股东大会、董事会、监事会议事规则以及董事、监事和高级管理人员的行为规范等	保荐机构督促奇安信依照相关规定健全完善公司治理制度，并严格执行公司治理制度
8	督导上市公司建立健全并有效执行内控制度，包括但不限于财务管理制度、会计核算制度和内部审计制度，以及募集资金使用、关联交易、对外担保、对外投资、衍生品交易、对子公司的控制等重大经营决策的程序与规则等	保荐机构对奇安信的内控制度的设计、实施和有效性进行了核查，奇安信的内控制度符合相关法规要求并得到了有效执行，能够保证公司的规范运行
9	督导上市公司建立健全并有效执行信息披露制度，审阅信息披露文件及其他相关文件，并有充分理由确信上市公司向上海证券交易所提交的文件不存在虚假记载、误导性陈述或重大遗漏	保荐机构督促奇安信严格执行信息披露制度，审阅信息披露文件及其他相关文件
10	对上市公司的信息披露文件及向中国证监会、上海证券交易所提交的其他文件进行事前审阅，对存在问题的信息披露文件及时督促公司予以更正或补充，公司不予更正或补充的，应及时向上海证券交易所报告；对上市公司的信息披露文件未进行事前审阅的，应在上市公司履行信息披露义务后五个交易日内，完成对有关文件的审阅工作，对存在问题的信息披露文件应及时督促上市公司更正或补充，上市公司不予更正或补充的，应及时向上海证券交易所报告	保荐机构对奇安信的信息披露文件进行了审阅，不存在应及时向上海证券交易所报告的情况
11	关注上市公司或其控股股东、实际控制人、董事、监事、高级管理人员受到中国证监会行政处罚、上海证券交易所纪律处分或者被上海证券交易所出具监管关注函的情况，并督促其完善内部控制制度，采取措施予以纠正	2021 年半年度，奇安信及其控股股东、实际控制人、董事、监事、高级管理人员未发生该等事项
12	持续关注上市公司及控股股东、实际控制人等履行承诺的情况，上市公司及控股股东、实际控制人等未履行承诺事项的，及时向上海证券交易所报告	2021 年半年度，奇安信及其控股股东、实际控制人不存在未履行承诺的情况
13	关注公共传媒关于上市公司的报道，及时针对市场传闻进行核查。经核查后发现上市公司存在应披露未披露的重大事项或与披露的信息与事实不符的，及时督促上市公司如实披露或予以澄清；上市公司不予披露	2021 年半年度，经保荐机构核查，奇安信不存在应及时向上海证券交易所报告的情况

	或澄清的，应及时向上海证券交易所报告	
14	发现以下情形之一的，督促上市公司做出说明并限期改正，同时向上海证券交易所报告：（一）涉嫌违反《上市规则》等相关业务规则；（二）证券服务机构及其签名人员出具的专业意见可能存在虚假记载、误导性陈述或重大遗漏等违法违规情形或其他不当情形；（三）公司出现《保荐办法》第七十一条、第七十二条规定的情形；（四）公司不配合持续督导工作；（五）上海证券交易所或保荐人认为需要报告的其他情形	2021 年半年度，奇安信未发生相关情况
15	制定对上市公司的现场检查工作计划，明确现场检查工作要求，确保现场检查工作质量。上市公司出现下列情形之一的，保荐机构、保荐代表人应当自知道或者应当知道之日起 15 日内进行专项现场核查：（一）存在重大财务造假嫌疑；（二）控股股东、实际控制人、董事、监事或者高级管理人员涉嫌侵占上市公司利益；（三）可能存在重大违规担保；（四）资金往来或者现金流存在重大异常；（五）上海证券交易所或者保荐机构认为应当进行现场核查的其他事项。	2021 年半年度，奇安信不存在需要专项现场检查的情形

二、保荐机构和保荐代表人发现的问题及整改情况

无。

三、重大风险

公司目前面临的风险因素主要如下：

（一）尚未盈利的风险

网络安全产品及技术研发以及销售和服务网络的搭建完善需要大量投入。报告期内，公司净利润为-92,505.74 万元，亏损较上年同期增加 30.40%，归属于上市公司股东的净利润-92,198.80 万元，亏损较上年同期增加 33.17%，归属于上市公司股东的扣除非经常性损益后的净利润-96,952.55 万元，亏损较上年同期增加 35.89%。截止 2021 年 6 月 30 日，公司累计未分配利润为-342,079.11 万元。公司持续亏损的主要原因是选择了高研发投入且人员快速扩张的发展模式，为建设研发平台、布局“新赛道”产品、提升攻防竞争力、建立全国应急响应中心而进行了大量投入。首先，研发平台聚焦核心技术能力的平台化输出，为安全产品提供共性核心能力，这些研发平台的开发具有周期长、投入高的特点；其次，公司核

心产品主要为网络安全领域的“新赛道”产品，开发这些产品要采用大量新技术，对研发人员能力要求高，增加了公司的研发投入；此外，公司在盈利模式的建设期仍需扩张研发团队和技术支持及安全服务团队，以期夯实规模性研发底座，向客户提供高质量的安全技术服务，积聚品牌效益，产生持续性商机，因此产生大量人员费用。本报告期内，公司尚未盈利且存在累计未弥补亏损，预计未来仍可能持续亏损，无法保证短期内实现盈利或进行利润分配。

（二）业绩大幅下滑或亏损的风险

2021 年上半年公司营业收入 14.56 亿元，同比增长 44.54%。公司未来能否保持持续成长，受到宏观经济、产业政策、行业竞争态势等宏观环境等因素的影响，同时公司未来经营业绩也取决于公司技术研发，产品市场推广及销售等因素。市场规模的变化、细分领域的市场竞争加剧、产品更新换代、新市场需求的培育等因素均可能导致下游市场需求发生波动。如果未来公司现有主要产品市场需求出现持续下滑或市场竞争加剧，同时公司未能及时培育和拓展新的应用市场，将导致公司主营业务收入、净利润面临下降的风险。公司将持续在产品研发、市场推广及销售等方面进行投入，如公司收入未能按计划增长，或规模效应未按预期逐步显现，则可能导致亏损进一步增加。如果上述影响公司持续成长的因素发生不利变化，且公司未能及时采取措施积极应对，则不能保证收入按计划增长，公司存在持续亏损的风险，将导致公司存在成长性下降或者不能达到预期的风险。

（三）核心竞争力风险

1、技术创新、新产品开发风险

公司所处的网络安全行业技术发展日新月异，行业发展趋势的不确定性，可能会导致公司在新技术的研发方向、重要产品的方案制定等方面不能及时做出准确决策，从而使公司新产品无法满足未来的行业需求，存在开发失败的风险。同时，技术创新及新产品研发需要投入大量资金和人员，通过不断尝试才可能成功，因此在开发过程中存在关键技术未能突破或者产品具体性能、指标、开发进度无法达到预期而研发失败的风险。此外，各种原因造成的研发创新及相应产品转化的进度拖延，也有可能造成公司未来新产品无法及时投放市场，对公司未来的市场竞争造成不利影响。

综上，公司在技术创新、新产品开发方面存在一定的风险。

2、核心技术泄密及核心技术人员流失的风险

当前公司多项产品和技术处于研发阶段，因此核心技术人员稳定及核心技术，保密对公司的发展尤为重要。在市场竞争中，一旦出现掌握核心技术的人员流失、核心技术信息失密、专利管理疏漏，导致核心技术流失，公司技术创新、新产品开发、生产经营将受到不利影响。

（四）经营风险

1、收入季节性波动的风险

公司客户主要来自于政府、公检法司、能源、金融、教育、医疗卫生、军队军工、运营商等领域，受上述最终客户预算管理和集中采购制度等因素影响，该部分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，收入主要集中于四季度，存在较为明显的季节性特征。又由于公司费用在年度内较为均衡地发生，而收入主要集中在第四季度，因此可能造成公司前三季度亏损较大的情况，公司收入和盈利有一定的季节性波动。

2、公司人员规模快速扩张，人力成本较高，可能对公司运营效率及管理效率造成不利影响

报告期末，公司销售、管理、研发费用占比较高。主要原因系公司为快速完成研发体系、产品体系、服务体系、销售及渠道体系等方面的建设和完善，快速扩张了人员规模。上述基础体系在建设期间并不能为公司带来直接的经济利益，因此造成了人力成本占营业总成本的比例较高，人员规模与收入规模短期内无法匹配的情况，对公司盈利能力、经营业绩造成不利影响。

3、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

公司作为网络产品、服务的提供者，在生产经营过程中应确保其提供的网络产品、服务符合相关标准并持续提供安全维护，在发现其网络产品、服务存在安全缺陷、漏洞等风险时应立即采取补救措施并履行相关告知和报告义务，涉及收集用户信息的应取得用户的同意并遵守个人信息保护的相关规定，如公司无法履

行该等义务，则有面临被有关主管部门责令改正、给予警告、没收违法所得或罚款等风险。此外，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。

4、研发投入占营业收入比重较高，持续资金需求较大的风险

一方面，公司以“数据驱动安全”为技术理念，重点建设了研发平台，聚焦核心技术能力的平台化输出，为安全产品提供共性核心能力，将安全产品需要的通用且核心能力平台化、模块化，避免了新产品研发过程中核心能力的重复研发，将极大降低未来新产品的研发成本及研发周期。但是上述研发平台的建设具有周期较长、投入较高的特性，需要公司投入大量的时间及资金进行开发、整合及完善，导致公司报告期内研发支出较高；另一方面，公司核心产品主要为网络安全领域的“新赛道”产品，如泛终端、新边界、大数据和云计算等安全防护产品，开发这些产品要采用大量新技术，对研发人员能力要求高，增加了公司的研发投入。目前，公司正在持续将安全产品围绕研发平台进行模块化改造，仍然有一定规模的研发投入需求；此外，网络安全行业与国际形势、技术发展、威胁变化均有较强的关联性，当攻防角色、模式或技术出现重大变化时，仍然需要进行较大的研发投入，客观上公司选择的发展模式仍然存在盈利周期较长的风险。

5、毛利率下降的风险

公司在系统集成性质的网络安全项目中向第三方采购的硬件，由于该等第三方硬件的市场较为成熟、价格相对透明，因此硬件及其他业务毛利率相对较低，使得该等业务收入的增长对发行人净利润贡献度较低。此外，由于集成类项目最终客户多为政企单位，受其预算管理和集中采购制度等因素影响，付款周期较长，对公司形成营运资金占用，并使得公司应收账款增加。未来，在政企单位信息化改造以及新基建建设过程中，公司仍可能承接系统集成性质的网络安全项目，使得公司主营业务毛利率存在下降的风险。

（五）行业风险

我国网络安全行业市场空间已颇具规模。随着我国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长；随着数字经济的发展，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。网络安全市场快速增长，也带来了较多参与者，网络安全市场快速增长，市场机遇也带来了较多参与者，竞争相对激烈。同时网络安全行业的快速发展，也会吸引更多的竞争者进军政企网络安全领域，公司可能面临市场竞争进一步加剧的风险。

公司来自政府等特定行业类客户收入占比较高，行业需求变化可能导致业绩产生波动报告期内，公司来自政府、公检法司及军队军工部门的收入占主营业务收入的比重超过 40%。近年来，该等行业客户的网络安全产品及服务需求主要由信息化投资加大、安全威胁加剧、网络安全监管趋严等因素驱动。未来，如因信息化投资增速、安全威胁程度、网络安全监管要求发生重大变化，可能导致该等行业客户的网络安全产品及服务需求发生波动，进而影响公司的经营业绩。如与当前行业发展趋势相反的情形，例如信息化投资放缓、安全威胁程度降低等持续出现，公司可能面临网络安全市场逐渐饱和、收入增速放缓。

（六）宏观环境风险

公司从事的网络安全等相关业务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。如果未来国家相关认证的政策、标准等发生重大变化，且公司未及时调整以适应相关政策、标准的要求，公司存在业务资质许可及产品、服务认证不能获得相关认证的风险。同时，若公司未来拓展的新业务需通过新的资质认定，且公司相关业务资质许可及产品、服务认证未能通过相关认证，将对公司开拓新市场造成不利影响。

公司享受的税收优惠包括企业所得税优惠、增值税退税及研发费用加计扣除。如果国家相关增值税税收优惠政策发生不利变化，或者公司未能如期收到增值税返还款项，将对公司经营成果产生不利影响。

若新冠肺炎疫情未能得到及时有效地控制，将可能导致公司无法及时向合作伙伴履约，无法对客户进行上门技术支持，客户的付款有所延迟等。该等情况均会对公司业务前景、研发计划、财务状况及经营业绩造成不利影响。

四、重大违规事项

2021 年半年度，公司不存在重大违规事项。

五、主要财务指标的变动原因及合理性

2021 年半年度，公司主要财务数据如下所示：

单位：元

项目	2021 年半年度	2020 年半年度	变动幅度（%）
营业收入	1,455,521,638.68	1,007,001,587.11	44.54
归属于上市公司股东的净利润	-921,987,958.39	-692,314,240.40	33.17
归属于上市公司股东的扣除非经常性损益的净利润	-969,525,497.26	-713,470,838.81	35.89
经营活动产生的现金流量净额	-1,268,465,136.34	-896,419,684.54	41.50
项目	2021 年 6 月 30 日	2020 年 12 月 31 日	变动幅度（%）
归属于上市公司股东的净资产	9,246,240,432.74	10,007,666,178.88	-7.61
总资产	13,083,690,351.51	12,424,319,146.93	5.31

2021 年半年度，公司主要财务指标如下表所示：

项目	2021 年半年度	2020 年半年度	变动幅度（%）
基本每股收益（元/股）	-1.36	-1.23	10.57
稀释每股收益（元/股）	-1.36	-1.23	10.57
扣除非经常性损益后的基本每股收益（元/股）	-1.43	-1.24	15.32
加权平均净资产收益率（%）	-9.58	-14.80	增加 5.22 个百分点
扣除非经常性损益后的加权平均净资产收益率（%）	-10.08	-15.26	增加 5.18 个百分点
研发投入占营业收入的比例（%）	52.68	54.23	减少 1.55 个百分点

2021 年半年度，公司主要财务数据及指标变动的原因如下：

1、报告期内，公司营业收入为 145,552.16 万元，同比增长率 44.54%，其中，主营业务 145,468.35 万元，同比增长率 45.34%。公司营业收入持续快速增长的主要原因，一方面是公司持续推进的“强研发”战略落地效果明显，核心产品市场竞争力全面提升，以实战化攻防能力带动产品和方案销售；另一方面，上半年

疫情稍有缓和，全行业数字化、智能化、云化转型加速，政府和企业客户的网络安全建设需求呈回暖态势。

2、报告期内，公司归属于上市公司股东的净利润-92,198.80 万元，亏损较上年同期增加 33.17%，归属于上市公司股东的扣除非经常性损益后的净利润-96,952.55 万元，亏损较上年同期增加 35.89%。公司经营活动产生的现金流量净额-126,846.51 万元，较上年同期减少 41.50%，主要系报告期内人员数量、薪资水平上涨导致支付给职工以及为职工支付的现金较去年同期有所增加所致。

3、报告期内，公司归属于上市公司股东的净资产较上年度末减少 7.61%，总资产较上年度末增加 5.31%。

4、报告期内，公司基本每股收益、稀释每股收益以及扣除非经常性损益后的基本每股收益较上年度同期有所减少，主要系报告期内公司亏损较去年同期扩大所致。

六、核心竞争力的变化情况

公司的核心竞争力主要体现在以下几个方面：

1、开创性的网络安全建设理念

公司开创性地提出了“内生安全”的核心理念，重塑网络安全体系，从过去的“局部整改”、“事后补救”的外挂式建设模式走向“深度融合”的体系化建设模式，改善网络安全体系化缺失、碎片化严重、协同能力差的旧有局面，构建全面的“事前防控”的新一代网络安全框架，与信息化过程同步规划、同步建设和同步运行，在信息化新建或改造中协助客户开展安全规划工作，扩大网络安全投入和产业规模，确保安全和信息化真正形成“一体化之两翼”、“双轮驱动”的效果。在“十三五”期间和目前进行中的“十四五”阶段，公司已为众多大中型客户有效开展了安全咨询和主动防御体系化规划，提升了网络安全在信息化投资中的预算占比，将网络安全作为数字化建设的基础性工作，夯实政企数字化信息化建设的安全底座，体现行业龙头的责任与担当。

在“内生安全—新一代网络安全框架”中，公司设计解构出了“十大工程、五大任务”，作为框架的具体落地指导，涵盖了当前所有的主流场景以及与技术

相关的信息化系统所需要的安全能力，通过 130 多个信息化组件、79 类网络安全组件的产品体系，覆盖了 29 个安全域场景。

2、强大的安全对抗技术

网络安全的核心是攻防对抗，公司已建成全链条以攻防为核心的技术能力体系。从漏洞挖掘与利用，到攻击检测与响应、恶意样本分析与查杀、威胁诱捕与反制、攻击追踪与溯源，再到威胁情报、全网攻击态势感知、APT 组织监控及电子取证等环节，均取得出色的成绩。

公司旗下拥有 A-TEAM、代码安全实验室、羲和实验室、观星实验室等多个攻防团队，帮助谷歌、微软、苹果、Oracle、Cisco、Juniper、Adobe、VMware、阿里云、华为、施耐德、以太坊等知名公司和组织修复安全漏洞，并屡次获得致谢。

公司应急响应部（奇安信 CERT）第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案，被 Oracle 评为了“在线状态安全性贡献者”，多次率先提供 WebLogic、Jackson 等重大安全问题的风险通告及可行的处置措施并获得官方致谢。

公司的威胁情报中心拥有大量的核心专业分析师和相应的数据运营和平台开发人员。公司的威胁情报中心专注于 APT 攻击类高级威胁的研究，其首发披露的 APT 组织超过 8 个。

公司代码安全实验室，基于自身漏洞挖掘和研究能力，支撑国家级漏洞平台的技术工作，多次向国家信息安全漏洞库（CNNVD）和国家信息安全漏洞共享平台（CNVD）报送原创通用型漏洞信息。

公司旗下的补天漏洞响应平台曾先后被公安部、国家信息安全漏洞共享平台(CNVD)、国家信息安全漏洞库(CNNVD)分别评定为技术支持先进单位、漏洞信息报送突出贡献单位和一级技术支撑单位。

3、强大的研发创新能力及平台能力

（1）强大的研发创新能力

公司在多个新安全技术领域中，研发并推出了一系列的具有技术创新优势的产品、方案和服务。在云安全、大数据安全、物联网安全、移动互联网安全、人工智能应用安全等新兴领域全面布局，并获得业界认可。

在云计算安全领域，公司掌握 VMware、KVM、Xen 三种平台的无代理杀毒和网络防护技术。公司凭借强大的云安全及安全服务能力，与腾讯云、阿里云、中国电子云等各类云平台服务商分别建立深度战略合作，预期在未来一起协同完成客户云场景的搭建及安全防护体系建设，实现数字政府、智慧城市等多领域的战略协同。

在终端安全领域，公司持续跟进客户所面对的安全风险，快速推出针对性解决方案。在 2020 年 1 月的 Win7 停服事件中，率先发布了 Win7 系统加固模块，为 Win7 和 Win Server 2008 的迁移和替换的过渡期保驾护航；在各种信创操作系统蓬勃发展的过程中，研发面向全平台的核心技术框架，在多样化的信创系统生态当中，获得了三大操作系统、五大 CPU 平台的兼容性认证，支持多种操作系统及超过 300 个内核版本；在终端管控上能够精准管控各类外接设备，积累形成了能够识别近 3 万款不同外接设备的信息数据库。

在大数据安全分析领域，公司充分利用人工智能技术进行安全分析，在数据挖掘、异常检测、复杂网络分析中都成功使用了深度学习和机器学习技术。

（2）强大的研发平台能力

当前，各类网络安全威胁与日俱增，新型攻击手段层出不穷，客户需求和场景千差万别，网络安全企业往往需要进行定制化开发新产品，并在一定程度上制约着网络安全产业的发展。为有效解决上述问题，公司逐步打造八大研发平台，避免了不同产品通用性的功能或模块的重复开发，极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品质量，更好满足政府、企业客户持续变化的个性化需求。

目前，公司全面布局“研发能力平台化”战略，以“鲲鹏”、“诺亚”、“雷尔”、“锡安”、“川陀”、“大禹”、“玄机”、“千星”八大网络安全研发平台为基础核心组件，再配合少量定制化特殊组件，快速研发满足客户定制化需求的网络安全产品和解决方案，大部分安全产品的研发周期将明显缩短。

4、全面丰富的网络安全产品体系

公司丰富的产品体系能够内生于客户的各个关键信息化领域，与其信息化环境进行深度融合与覆盖，形成有效的、系统性的防护。报告期内，根据 2021 年 3 月安全牛发布的第八版中国网络安全行业全景图，公司的产品线覆盖 13 个一级安全领域和 94 个二级细分领域，连续多年蝉联入选全景图细分领域最多的企业。

公司自研的安全产品帮助客户实现以安全大数据为核心，威胁情报驱动的多品类协同联动的主动防御体系。主动防御体系更具备实战化效果，故攻防实战化演习让公司的实战化产品及方案在市场竞争中脱颖而出。

除此之外，公司在零信任身份安全、代码开发安全、工业互联网安全、智能网联车安全、大数据安全隐私保护及安全教育等多个创新赛道积极布局，助力公司在报告期内新赛道品类竞争力明显提升。

5、强大的安全咨询规划、实战攻防、安全运营与应急响应服务能力

（1）强大的咨询规划服务能力

公司针对“十四五”规划、新基建与数字化转型，以系统工程方法，结合政企大型机构的业务战略与信息化战略，为政企机构梳理网络安全战略目标。公司以“内生安全框架”体系规划设计方法与工具，从技术、管理和运行等多个视角，为政企机构进行网路安全能力体系的梳理。同时，公司秉承着“同步规划、同步建设、同步运营”与网络安全“关口前移”的思想，在客户信息化、数字化的体系规划设计阶段，就同步进行网络安全体系规划，向客户输出网络安全中长期规划设计，帮助政企构建动态综合的网络安全防御体系及实战化运行体系，为政企数字化业务发展保驾护航。

公司已为政府、部委、重点央企、金融、智慧城市/数字政务、大型制造业等近百家大型机构进行了“十三五”、“十四五”、3-5 年期网络安全体系规划设计，完成输出了“新一代网络安全框架”白皮书、方法论、配套工具集，对重点行业的“十四五”网络安全规划产生重要牵引作用。

（2）强大的实战攻防服务能力

2020 年，在国家级的年度网络攻防演习中，公司成绩均名列前茅，在累计200余家参加演习的单位中，超过60%单位聘请公司作为主力防护队伍；在各省、部级部门组织的网络攻防演习中，由公司承办、参与的超过 200 场，得到了客户的广泛认可。

在漏洞报告和响应方面，公司建立的“补天漏洞平台”是 2017-2020 年对 CNVD 漏洞共享平台贡献最多的中文漏洞响应平台，四年来累计为 CNVD 报送漏洞数十万个，补天漏洞响应平台已成为重要机构和企事业单位漏洞响应的重要保障力量。

（3）全天候、全覆盖的安全运营与应急响应服务能力

公司作为主要技术保障单位已先后完成了国庆 70 周年、澳门回归 20 周年、亚洲文明对话大会、“一带一路”高峰论坛、海军建军 70 周年、全国两会、春晚、中非合作论坛、上合组织成员国峰会、十九大、博鳌论坛、2020 服贸会等国家级网络安全保卫任务。除此以外，公司为社会各政企单位提供全天候 24 小时的网络安全应急处置服务，保障了众多政企机构及大中型企业信息系统的正常运营。用自己的能力和行动捍卫着国家和企业的网络安全。

公司建设场景化安全运营能力，在系统安全、网络安全策略、检测与分析、云安全、安全管理、态势感知等多个领域，通过一线驻场与二线专家相结合的模式，设计场景化的安全运营体系，为政企单位提供了持续的安全运营保障。

6、优质的客户群、丰富的行业经验和完善的营销体系

公司客户范围已覆盖大多数中央政府部门、中央直属企业和银行以及全行业的客户单位。此外，公司在长期为政企客户提供服务的过程中，深入了解客户的需求演变、不同行业的需求差异，积累了大量深厚的产品、服务和交付经验。伴随着公司攻防技术、大数据技术及人工智能技术的不断发展，能为客户提供契合度高的网络安全解决方案，高质量的满足客户的需求。广泛而优质的客户群为公司新产品、新方案、新服务的推广和既有产品及服务向其他领域的覆盖提供了坚实的基础，是公司持续健康发展的有力保证。

公司形成了较为完善的营销服务体系，具有网络覆盖面广和服务响应及时的

优势，成为提高和巩固公司市场竞争力的重要因素之一。

7、网络安全领域的著名品牌

经过多年的发展，奇安信已经成为网络安全领域的著名品牌。公司是北京2022 年冬奥会和冬残奥会组委会官方网络安全服务和杀毒软件赞助商，成为了具有国际影响力的安全品牌；公司每年举办的“北京网络安全大会”已成为亚太地区最专业的、规模最大的网络安全盛会之一，大会“内生安全”的主题思想成为网络安全产业发展的风向标；目前，公司旗下“补天漏洞响应平台”拥有超过7万名白帽子注册会员，累计提交漏洞数量已超过50万个，漏洞影响企业数12000余家，入驻企业 5900 多家，已成为全球最知名的网络安全社区之一；“奇安信威胁情报中心”专注于 APT 攻击类高级威胁的研究，已成为全球最知名的 APT 研究组织之一。

8、优秀人才团队和良好的企业文化

公司把人才培养和组织能力建设作为一项战略投资，通过一系列有效的聘用、培养和激励机制保障团队稳定。公司对人员培养持续投入，保证源源不断的人才供给和内部人员的能力提升。去年，公司进一步健全公司长效激励约束机制，制定了 2020 年度限制性股票激励计划并向 1,147 名公司管理人员、核心技术人员及其他员工授予了限制性股票，有效地将股东、公司和核心团队三方利益结合在一起，使各方共同关注公司的长远发展，以确保公司发展战略和经营目标的实现。

上述公司的核心竞争力在 2021 年半年度未发生不利变化。

七、研发支出变化及研发进展

为了保证公司能够不断进行技术创新，保持产品和服务的技术领先水平，维持公司的市场竞争优势，公司持续进行研发投入。2021 年半年度，公司研发费用投入金额为 7.67 亿元，较上年同期上升 40.40%，主要原因系报告期内研发人员数量、薪资水平上涨导致薪酬增加，且本期较去年同期新增股份支付费用，此外，随着研发项目不断深入，使得相关资源投入增加所致。研发费用占公司营收比重由 2020 年半年度的 54.23%降至 2021 年半年度的 52.68%，占比小幅下降。

八、新增业务进展是否与前期信息披露一致

不适用。

九、募集资金的使用情况及是否合规

截至 2021 年 6 月 30 日止,公司募集资金使用情况如下:

项目	金额（元）
募集资金总额	5,718,922,581.90
减：发行费用	307,067,554.76
募集资金净额	5,411,855,027.14
加：存款利息和现金管理收益扣除银行手续费等净额	56,754,613.59
减：直接投入募投项目的金额	1,556,841,860.64
临时补流资金	1,030,000,000.00
截至 2021 年 6 月 30 日募集资金余额	2,881,767,780.09

截至 2021 年 6 月 30 日，奇安信募集资金存放和使用符合《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》、《上海证券交易所科创板股票上市规则》等法规和文件的规定，对募集资金进行了专户存储和专项使用，并及时履行了相关信息披露义务，募集资金使用不存在违反相关法律法规的情形。

十、控股股东、实际控制人、董事、监事和高级管理人员的持股、质押、冻结及减持情况

截至 2021 年 6 月 30 日，现任及报告期内离任董事、监事、高级管理人员和核心技术人员持股变动情况如下表所示：

姓名	职务(注)	上年度末持股数	期末持股数	半年度内股份增减变动量	增减变动原因
齐向东	董事长	149,561,640	149,561,640	-	-
吴云坤	董事、总裁	-	-	-	-
姜军成	董事	-	-	-	-
杨洪鹏	董事、副总裁	-	-	-	-

孟焰	独立董事	-	-	-	-
徐建军	独立董事	-	-	-	-
赵炳弟	独立董事	-	-	-	-
韩洪伟	监事会主席	-	-	-	-
张嘉禾	职工代表监事	-	-	-	-
王欣	监事	-	-	-	-
刘红锦	财务总监	-	-	-	-
何新飞	副总裁	-	-	-	-
徐贵斌	副总裁	-	-	-	-
左文建	副总裁	-	-	-	-
马勒思	董事会秘书	-	-	-	-
马江波	大数据与安全运营业务线总经理	-	-	-	-
刘浩	云安全业务线总经理	-	-	-	-
刘岩	智能安全网络事业部副总经理	-	-	-	-
吴勇义	大数据与态势感知业务线技术总监	-	-	-	-
顾永翔	终端安全业务线副总经理	-	-	-	-
吉艳敏	终端安全业务线技术总监	-	-	-	-
樊俊诚	智能安全网络事业部副总经理	-	-	-	-
叶盛	大数据与态势感知业务线架构师	-	-	-	-
汤迪斌	终端安全业务线产品总监	-	-	-	-
合计	/	149,561,640	149,561,640	-	/

注：1、吴云坤通过天津奇安壹号科技合伙企业（有限合伙）、宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）间接持有公司 2.79%的股权。2、何新飞通过天津奇安壹号科技合伙企业（有限合伙）间接持有公司 0.29%的股权。

截至 2021 年 6 月 30 日，奇安信控股股东、实际控制人和董事、监事和高级管理人员持有的奇安信股份均不存在质押、冻结及减持的情形。

十一、上海证券交易所或保荐机构认为应当发表意见的其他事项

截至本持续督导跟踪报告出具之日，不存在保荐机构认为应当发表意见的其

他事项。

（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奇安信科技集团股份有限公司 2021 年半年度持续督导跟踪报告》签字盖章页）

保荐代表人：

董军峰　　李彦斌

中信建投证券股份有限公司

2021 年 9 月 1 日