西部证券股份有限公司
关于北京信安世纪科技股份有限公司
2023 年度持续督导跟踪报告

根据《证券发行上市保荐业务管理办法》《上海证券交易所科创板股票上市规则》等有关法律、法规的规定，西部证券股份有限公司（以下简称“保荐机构”）作为北京信安世纪科技股份有限公司（以下简称“信安世纪”、“公司”）持续督导工作的保荐机构，负责信安世纪上市后的持续督导工作，并出具本持续督导跟踪报告。

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。	保荐人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，与上市公司或相关当事人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。	保荐人已与信安世纪签订承销与保荐协议，该协议明确了双方在持续督导期间的权利和义务，并报上海证券交易所备案。
3	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。	保荐人通过日常沟通、定期或不定期回访、现场检查等方式，了解信安世纪业务情况，对信安世纪开展持续督导工作。
4	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。	2023 年度，信安世纪在持续督导期间未发生按有关规定须保荐人公开发表声明的违法违规情况。
5	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。	2023 年度，信安世纪在持续督导期间未发生违法违规或违背承诺等事项。
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，并切实履行其所做出的各项承诺。	2023 年度，保荐人督导信安世纪及其董事、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。	保荐人督促信安世纪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。	保荐人对信安世纪的内控制度的设计、实施和有效性进行了核查，信安世纪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。

序号	工作内容	持续督导情况
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。	保荐人督促信安世纪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。	保荐人对信安世纪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了事前审阅，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，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。	2023 年度，信安世纪及其控股股东、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。	2023 年度，信安世纪及其控股股东、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；上市公司不予披露或澄清的，应及时向上海证券交易所报告。	2023 年度，本持续督导期间，信安世纪未出现该等事项。
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。	2023 年度，信安世纪未发生前述情况。
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。	保荐人已制定了对信安世纪的现场检查工作计划，并明确了现场检查工作要求，确保现场检查工作质量。
16	上市公司出现以下情形之一的，保荐人、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。	2023 年度，信安世纪不存在前述情形。

二、 保荐人和保荐代表人发现的问题及整改情况

无。

三、 重大风险事项

公司目前面临的风险因素主要如下：

（一）业绩大幅下滑或亏损的风险

1、业绩大幅下滑的具体原因

报告期内，公司在深耕现有金融、烟草、交通、人社等传统优势行业的基础上，加大对教育、医疗等行业的拓展，积极探索无人机等领域的新应用，并加强产品在 IPV6 网络环境下的实现，但受宏观经济等因素影响，部分客户采购节奏延缓，订单签订、项目交付、验收等环节出现不同程度的延期，公司实现营业收入 54,922.69 万元，同比降低 16.54%。为保证高质量长远发展，公司持续研发、技术、市场等方面的人才储备，员工人数及薪酬同比增长，公司实现归属于母公司所有者的净利润 1,122.27 万元，同比降低 93.15%。

2、主营业务、核心竞争力及所处行业景气情况

近年来，国际、国内重大网络安全事故频发，我国对网络信息安全的重视程度不断提高，金融、政府及大型企业对网络安全产品的需求不断提升。同时，商用密码的应用领域亦从金融、财政、烟草、交通、通信、政务等重要应用领域医疗、教育、农业等新的应用领域拓展。随着云计算、移动互联网、物联网、车联网、工业互联网等新业态、新应用、新场景的不断涌现，针对新技术环境下的数据安全和隐私保护等问题，都对网络安全和密码安全提出了新需求。网络安全和商用密码市场仍将保持快速发展态势。报告期内，公司主营业务、核心竞争力均未发生重大不利变化，与网络安全和商用密码行业整体趋势一致。

（二）核心竞争力风险

1、产品迭代无法适应市场发展需求的风险

报告期内，公司业务主要围绕网络应用安全展开，如果网络应用市场急剧变化，公司不能做出快速响应、精准把握和前瞻性判断，产品迭代升级跟不上市场的需求，公司将会受到行业内有竞争力的企业和竞争产品的冲击，对公司持续经营能力造成不利影响。

2、核心技术人员流失及技术泄露风险

公司所处行业是知识密集型的行业，掌握核心技术并保持核心技术团队稳定是保持公司核心竞争力及未来持续发展的基础。当前市场各厂商间对于技术和人才竞争日益激烈，若公司未来无法为技术人员提供具备竞争力的薪酬水平、激励机制和发展空间将可能导致核心技术人员流失，对公司的技术研发以及生产经营造成不利影响

（三）经营风险

受客户结构、业务特点等因素的影响，公司营业收入和利润水平存在季节性分布不均衡的特点，下半年的营业收入和利润水平占全年的比例高于上半年,但员工工资、研发费用、固定资产折旧等各项费用在年度内发生则相对均衡，公司经营业绩存在季节性波动风险。

（四）财务风险

公司营业收入具有季节性特征，销售收入集中在下半年尤其是第四季度，导致公司的营运资金周转压力加大；如果公司主要客户的财务经营状况发生重大不利变化，将进一步加大公司坏账损失的风险，进而对公司资产质量以及财务状况产生不利影响。

（五）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，细分行业较多，未来，随着网络信息安全行业的发展，各细分领域的技术将会融合、协同，各细分市场客户的需求将会交叉、重叠，对参与者提供整体解决方案的能力将提出更高的要求，各细分行业的领先者将展开直接竞争，导致竞争进一步加剧；其他行业有竞争优势的企业可能进入网络信息安全行业，进而导致行业整体竞争加剧。同时，网络信息安全行业保持快速发展基于目前国家政策、全球信息安全形势和新技术技术发展方向，一旦外部因素发生重大变化，或者客户需求发生变化，可能导致信息安全行业发展不及预期。如上行业存在的风险可能影响公司经营业绩。

（六）宏观环境风险

国家一直重视高新技术企业，并给予重点鼓励和扶持。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。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和相关扶持政策发生变化，则可能对公司发展产生一定的影响。

另外，公司面向的金融、政府、大型企业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，宏观经济环境如出现不景气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不利影响。

四、 重大违规事项

2023 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

2023 年度，公司主要财务数据及指标如下所示：

单位：人民币元

主要会计数据	本报告期	上年同期	增减变动幅度（%）
营业收入	549,226,850.31	658,076,109.27	-16.54
归属于上市公司股东的净利润	11,222,676.59	163,924,540.37	-93.15
归属于上市公司股东的扣除非经常性损益的净利润	9,466,995.69	155,548,322.01	-93.91
经营活动产生的现金流量净额	40,168,032.39	72,870,758.88	-44.88
	2023 年末	**2022 年末**	**本期末比上年同期末增减（%）**
归属于上市公司股东的净资产	1,378,711,115.63	1,152,821,656.32	19.59
总资产	1,585,547,276.30	1,328,770,448.71	19.32

主要财务指标	2023 年	2022 年	本期比上年同期增减(%)
基本每股收益（元 / 股）	0.0532	1.1893	-95.53
稀释每股收益（元 / 股）	0.0532	1.1893	-95.53
扣除非经常性损益后的基本每股收益（元 / 股）	0.0449	0.7625	-94.11
加权平均净资产收益率（%）	1.95	15.88	-13.93
扣除非经常性损益后的加权平均净资产收益率（%）	1.81	15.11	减少 13.30 个百分点
研发投入占营业收入的比例（%）	35.3	20.32	增加 14.98 个百分点

上述主要财务指标的变动原因如下：

2023 年度，公司实现营业收入 54,922.69 万元，与上年同期相比减少 16.54%；实现归属于母公司所有者的净利润 1,122.27 万元，同比减少 93.15%；实现归属于母公司所有者的扣除非经常性损益的净利润 946.70 万元，同比减少 93.91%。

报告期内，公司财务状况良好，资产规模稳定增长，2023 年末总资产为 158,554.73

万元，同比增长 19.32%；归属于母公司的所有者权益 137,871.11 万元，同比增长 19.59%。

报告期内，公司在深耕现有金融、烟草、交通、人社等传统优势行业的基础上，加大对教育、医疗等行业的拓展，积极探索无人机等领域的新应用，并加强产品在 IPV6 网络环境下的实现，但受宏观经济等因素影响，部分客户采购节奏延缓，订单签订、项目交付、验收等环节出现不同程度的延期，公司实现营业收入 54,922.69 万元，同比下降 16.54%；

报告期内，公司持续加大研发投入，支付给职工以及为职工支付的现金较上年同期增长，导致经营活动产生的现金流量净额减少 44.88%。

六、 核心竞争力的变化情况

公司始终将技术研发作为公司的业务核心，重视技术开发和技术创新工作，报告期内公司通过持续加大研发投入、引进研发人才，不断完善研发管理体系等方式保持核心竞争力。经过多年的积累，公司在密码行业中具有相对较强的技术与研发优势，截至报告期内，目前公司主要产品中的核心技术、技术来源均为自主研发、技术创新类型均为原始创新，技术特点和技术成熟度等方面的具体情况如下：

序号	技术名称	技术特点	相关产品与服务	所处阶段
1	网络密钥安全派生与协同签名技术	采用独创的移动端密钥防护和存储技术实现移动端派生密钥和数据安全存储，以及独创的算法和协议实现移动端派生密钥和服务端密钥的协同签名技术。	移动安全认证系统、云密码安全服务平台系统	成熟稳定
2	基于人工智能的用户行为分析鉴别技术	通过用户行为大数据信息，利用机器深度学习，采用独创的学习算法和大数据快速分析技术实现用户身份鉴别与行为风险分析。	移动安全认证系统、云密码安全服务平台系统	成熟稳定
3	网络传输加密与处理技术	通过独创的协议优化以及算法，对应用数据在网络传输和存储过程中进行加解密处理技术。	NSAE 应用安全网关、应用安全网关系统、NetOpti 应用交付系统、NetGate SSL VPN 网关、NetSafe 安全互联网关	成熟应用
4	基于安全套接层协议特征的加速负载分发技术	独创的基于压缩、缓存、安全套接层协议优化在内的服务器加速负载分发技术。	NSAE 应用安全网关、应用安全网关系统、NetOpti 应用交付系统、NetGate SSL VPN 网关、NetSafe 安全互联网关	成熟稳定
5	云架构密码分发与权限控制技术	采用独创的云架构虚拟化环境下密钥存储和权限控制技术实现云端密码管控。	移动安全认证系统、CCypher 云密码服务平台	成熟稳定成熟应用
6	数字证书与加密协议格式的快速解析和判定技术	通过独创的解析算法对数字证书以及签名加解密格式进行快速解析分析和判定。	NetCert 证书认证系统、NetPass 动态密码系统、NetAuth 统一身份认证管理系统、NetSign 签名验签服务器、NetSeal 电子签章系统	成熟稳定

7	移动威胁态势感知技术	通过本技术提供的分析引擎和算法库，实现对移动操作系统漏洞、开放端口、黑客入侵、web 攻击、APP 攻击、威胁情报、企业安全舆情等全方位的监控，及时预警或预测威胁态势。	移动安全认证系统、CCypher 云密码服务平台	成熟稳定
8	高性能动态可配置的 API 网关技术	在 API 网关统一解决微服务集群的认证、鉴权、流量管控、熔断、灰度发布等问题，提升运维管控效率，在保障系统安全接入的基础上，构建高性能、高可靠稳定运行能力。	NetCert 证书认证系统、NetPass 动态密码系统、NetAuth 统一身份认证管理系统、NetSign 签名验签服务器、NetSeal 电子签章系统	成熟稳定
9	基于时序数据库分布式业务监控技术	采用特殊数据存储和索引方式，可以高效存储和快速处理海量时序大数据。相对于关系型数据库它的存储空间减半，查询速度极大的提高。时间序列函数优越的查询性能远超过关系型数据库，非常适合在监控预警分析领域的应用。	CCypher 云密码服务平台	成熟稳定
10	高效安全的容灾技术和集群技术	通过对硬件安全产品密钥运算主运算卡与多个待同步运算卡快速协同同步技术以及数据网络镜像技术，实现了运算卡密钥及安全配置数据等容灾和集群技术，同时保证产品的高性能、稳定性和可靠性。	NetCert 证书认证系统、NetPass 动态密码系统、NetAuth 统一身份认证管理系统、NetSign 签名验签服务器、NetSeal 电子签章系统	成熟稳定
11	高性能网络产品架构技术	使用独创的 SpeedStackTM 专利技术，实现了快速 TCP/IP 协议栈、应用代理和智能应用协议分析器，保证产品的高性能、稳定性和可靠性。	NSAE 应用安全网关、应用安全网关系统、NetOpti 应用交付系统、NetGate SSL VPN 网关、NetSafe 安全互联网关	成熟稳定
12	智能流量学习和应用识别技术	利用智能流量学习和应用识别技术，对网络流量进行分析建模，对各类网络应用进行识别，精准判断攻击流量，准确封堵攻击源头，为企业网络提供安全保障。	NSAE 应用安全网关	成熟稳定
13	远程安全接入技术	通过独创的软件虚拟化技术和严格的逻辑隔离技术，使得单个硬件设备最大支持 256 个虚拟服务站点和最大 128,000 并发用户。	NetGate SSL VPN 网关	成熟稳定

14	零信任边界安全保护技术	通过独创的 URL 和内容改写技术，无缝透明代理并保护后台的边界内应用。通过独创的 AAA 代理技术，为边界内的应用提供身份认证、预授权、集中审计的安全加固。	NetGate SSL VPN 网关、NetOpti 应用交付系统	成熟稳定
15	网络设备虚拟化平台管理技术	使用自研的虚拟化管理技术，为各种不同种类的虚拟化网络设备提供统一的 NFP 平台，从而实现与云计算匹配的弹性网络配置，灵活资源管理，并提供高性能以及高可用性的网络虚拟化平台。可广泛用于各种私有云，公有云以及混合云的部署场景。	CCypher 云密码服务平台	成熟稳定
16	网络虚拟化平台的性能优化	在虚拟化平台中使用多种独创的网络性能优化技术，提升加解密运算和网络转发性能，从而解决传统云计算和 NFP 平台网络性能和加解密性能低的核心问题，实现大容量和高并发的网络虚拟化平台。	CCypher 云密码服务平台	成熟稳定
17	数据安全隐私保护技术	以密码技术为核心，结合信息技术和相关应用场景，构建数据安全隐私保护的基础技术平台，进而构建支持隐私计算、机器学习的一体化平台	NetMPC 隐私计算平台	新技术探索
18	多方安全计算技术	利用密码技术，在保护个人隐私的前提下进行协同计算，平衡数据使用中“可用性”和“隐私性”之间的矛盾，广泛应用于隐私计算场景中	NetMPC 隐私计算平台	新技术探索
19	一种基于滑动窗口的高容错无反馈链路影像传输方法及系统	根据滑动窗口冗余信息，进行跳步解码；去除冗余数据，实现物理隔离情况下无反馈链路的信息单向传输。本系统以滑动窗口策略进行冗余数据传输，以跳步策略避免多余图形解码，能提升无反馈链路信息传输的高容错性	影像交换系统	成熟稳定应用

20	一种基于标志帧的低功耗单向无反馈影像传输方法及系统	发送端将程序启动、准备发送数据、结束发送数据状态制作成启动帧、准备帧、结束帧特殊标志的影像，将这些特殊标志影像推送到显示终端显示；接收端采集影像数据，解析出影像数据标识出帧类型判断出发送端当前状态；根据系统所属的不同工作状态切换发送端显示终端、接收端采集模块的工作模式；降低单向无反馈影像传输系统显示终端和采集模块功耗以及延长其使用时间	影像交换系统	成熟稳定应用
21	一种集中文印的用户自助交互终端以及方法	集中文印的用户自助交互终端以及方法，能够实现集中文印室的无人值守，可采用分布式部署支持多文印室就近文件打刻，改变原打印机加装刷卡器的哑终端模式，并支持一带多模式，有效控制使用成本；采用分布式文件服务和集中输出服务，能够完成多点部署，配合集中文印系统实现就近文件打印，避免复杂网络拓扑、物理分散情况下的不必要的网络传输	集中文印系统、文印交互终端	成熟稳定应用
22	一种高效的光盘刻录打印方法及装置	该光盘刻录打印方法包括采用免编程的基于SAMBA 方式对外接口，只需要映射完成就可以直接提交刻录打印任务；支持多用户并发提交任务，避免排队等待；光盘刻录打印装置采用多光驱支持多个任务并发，涉及到避免抓盘机械手与多光驱干涉问题；采用暂存仓进行提前刻录打印，避免排队等候，采用刷卡、指纹等多种身份验证防止光盘误取导致失泄密。本发明方案完成多用户、多任务的光盘并发刻录打印，能够极大提升刻打效率，节约用户等待时间	集中文印系统、光盘刻打一体机	成熟稳定应用

七、 研发支出变化及研发进展

（一） 研发支出及变化情况

单位：人民币元

项目	本年度	上年度	变化幅度（%）
费用化研发投入	193,878,024.86	133,709,633.35	45.00%
资本化研发投入	-	-	-
研发投入合计	193,878,024.86	133,709,633.35	45.00%
研发投入总额占营业收入比例（%）	35.30	20.32	增加 14.98 个百分点
研发投入资本化的比重（%）	-	-	-

报告期内，公司持续加大研发投入，扩充研发队伍，使职工薪酬总额有较大幅度提高，导致研发费用增长较快。

（二） 研发进展

单位：万元

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
1	可信数字信任体系研发升级项目	4,000.00	3,889.60	3,889.60	1）完善身份认证安全系统：升级产品架构，支持云架构部署下的身份认证系统部署运维管理，支持多算法多服务，支持新一代软硬件平台，支持国家标准升级的产品功能增强。2）升级智能网联汽车交通认证系统：支持隐私证书和无证书，支持异常行为管理机构，支持十亿级别证书与密钥存储，支持新一代软硬件平台。3）升级统一身份管理系统：完善零信任相关功能特性，升级微服务架构，优化业务流程，支持新一代软硬件平台。4）创新实现智能化零信任动态策略中心。	1）完善身份认证安全系统，实现身份认证系统升级，支持云架构部署；支持多算法多服务，支持新一代软硬件平台。2）智能网联汽车身份认证方案与产品升级。3）完善统一身份管理系统具备零信任特性。实现零新人动态策略中心的 AI 智能化权限与认证判别。	1）身份认证安全系统产品在遵循国家、国际相关 PKI 标准规范的基础上，全面支持国产算法和国际算法及其协议标准规范。2）智能网联汽车认证系统管理；支持十亿级别证书与密钥存储。3）统一身份管理系统具备零信任动态策略评估特性。	1）支持新技术/新架构对产品的应用需求：云架构、移动化、区块链、隐私计算、零信任等。2）支持新的应用场景：物联网、车联网、数字货币、CIPS、证券、期货、基金、医疗、无人机等。
2	数据安全防护研发升级项目	3,000.00	2,763.65	2,763.65	1）完善签名服务器产品：升级产品架构，支持新一代软硬件平台，支持移动化、云架构新兴应用场景，安全性提升，推出安全三级的签名服务器产品。完善时间戳服务器时间源与功能的深度集成。支持新一代软硬件平台，性能提升。 2）实现签章产品升级：完善自助服务流程，完善签章客户端，支持多平台、多业务场景、多文件格式签章，支持新一代软硬件	1）完善数据安全系列产品实现签名服务器、签章服务器、TSA 时间戳产品升级。2）数据加解密服务系统产品能够实现业务系统无感知情况下的数据加密，不影响应用访问。3）新增密码机	1）签名服务器产品达到安全三级。时间戳服务器时间源与功能的深度集成。 2）签章产品支持多平台、多业务场景、多文件格式签章。 3）数据加解密服务系统产品能够实现业务系统无感知情况下的数据加密，不影	1）支持新技术/新架构对产品的应用需求：云架构、移动化、区块链、隐私计算、零信任等。2）支持新的应用场景：物联网、车联网、数字货币、CIPS、证券、期货、基金、医疗、无人机等。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
					平台；3）升级数据加解密服务系统产品：支持新一代软硬件平台，性能提升，完善多场景、多语言、多架构下透明加解密能力。支持实现属性加密、保留格式加密等新型防护密码技术。4）新增密码机、云密码机产品	云密码机等密码产品。	响应用访问。4）云密码机支持 VSM 间密钥隔离、海量密钥管理、虚拟化等技术	
3	信创高能网络安全系列产品升级项目	3,000.00	2,613.13	2,613.13	1）实现 NSAE 应用安全网关/NetOpti 应用交付系统产品升级：支持信创新一代硬件平台，优化软件架构设计，优化网络调度算法以及流量控制，支持 HTTP3/QUIC 等新协议，提升健康检查功能增强与易用性，推出安全三级的网关产品。 2）完善零信任安全网关：增强零信任安全能力，支持 IPv4&IPv6 双栈，提升易用性和安全性，安全可视化。3）完善应用安全防火墙产品：支持新一代硬件平台，优化软件架构设计，增强数据流量分析、应用控制、入侵检测和防范，提升动态安全和 API 安全能力。	1）实现 NSAE 应用安全网关产品升级；实现 NetOpti 应用交付系统升级。2）完善零信任安全网关，构建以身份为边界的零信任安全模式。3）完善应用安全防火墙产品。	1）通信安全产品实现算法与安全协议优化，对应用数据在网络传输和存储过程中进行加解密快速处理。2）NSAE 应用安全网关产品达到安全三级。3）零信任产品以商用密码技术和为核心，融合采用 SDP 软件定义边界技术、IAM 身份识别与访问管理技术等零信任技术，构建以身份为边界的零信任安全模式。	1）支持新技术/新架构对产品的应用需求：云架构、移动化、区块链、隐私计算、零信任等。2）支持新的应用场景：物联网、车联网、数字货币、CIPS、证券、期货、基金、医疗、无人机等。
4	移动安全系列产品升级项目	1,200.00	1,095.00	1,095.00	1）完善移动安全认证平台，实现移动安全认证系列产品升级改造：升级产品架构，提升性能，提升管理功能与易用性。增强移动安全客户端功能与安全性。	1）针对移动互联网轻量化信息安全要求，开发相应的信息移动安全产品。	1）移动安全认证平台通过架构优化、算法优化支持高效的协同签名算法及多种协同签名模式，可无缝对接支持目前主流移动框架。	1）支持新的应用场景：物联网、车联网、数字货币、CIPS、证券、期货、基金、医疗、无人机等。

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
5	云原生密码安全产品项目及项目	7,300.00	7,096.44	7,096.44	1）完善密码应用一体化系统：支持新一代软硬件平台，增强 Kubernetes 功能，增强分布式存储能力。 2）新增密码安全服务管理平台产品，实现密码设备资源池的弹性调度管理、典型密码应用服务的发布与管理、租户化管理与计费等功能的一体化密码云管理平台。 3）新增云服务器密码机，完善虚拟化技术，支持多个虚拟服务器密码机同时提供服务,并保持各个虚机物理设备资源、密码运算资源等部件的共享与安全隔离。	1）以云计算技术为基础，针对云计算的信息安全要求进行产品开发。 2）云服务器密码机产品作为云数据中心必要的基础安全资源。	1）密码安全服务管理平台全面覆盖公有云模式、混合云模式、多云架构模式等复杂场景。 2）云服务器密码机支持多个虚拟服务器密码机同时提供服务,并保持各个虚机物理设备资源、密码运算资源等部件的共享与安全隔离。	1）支持新的应用场景：物联网、车联网、数字货币、CIPS、证券、期货、基金、医疗、无人机领域等。
6	安全监管合规服务平台项目	2,000.00	655.29	655.29	1）完善全密码安全服务平台产品：完善密码资源池管理，提升性能，完善密码全流程应用态势感知。2）新增密码安全可视化监管系统：完善监控指标与告警流程；新增密码设备管控，提高可视化管控能力，提升易用性。	1）实现全密码安全服务总线，为各类业务数据流动提供统一的安全机制。2)安全可视化监管系统实时监控密码应用设备的状态、密码服务的状态以及代理状态的监控以及密码应用日志的集中审计。	1）全密码安全服务平台实现密码应用行为的全生命周期管理与服务。 2）安全可视化监管系统采用多种主动探测技术，实现实时可视化监控。	1）支持新的应用场景：物联网、车联网、数字货币、CIPS、证券、期货、基金、医疗、无人机领域等。2）应对各行业安全监管需求场景。
7	新兴领域研发	500.00	303.41	303.41	1）新增视频安全一体机：用于视频监控数据完整性保护，能够帮助用户满足视频监控的安全要求，保证视频安全合规。2）完善隐私计算算法研	1）视频安全一体机产品专门用于视频监控数据完整性保护的产品，能够帮助	1）视频安全一体机产品支持主流摄像头，支持国家、国内标准视频传输协议和主流厂商	1）支持视频监控安全。 2）数据要素共享确权领域支持隐私计算。3）多行业后量子

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
	项目				究并申请相关专利，提升隐私计算算法性能，完善安全多方计算平台产品。3）新增后量子密码研究，完成后量子密码算法验证。	用户满足视频监控的安全要求。 2）完善隐私计算平台，提升隐私计算性能 3）实现后量子密码产品与金融行业迁移方案。	的私有协议。 2）隐私计算支持主流隐私计算算法。3）NIST 后量子密码算法产品支持。	密码算法迁移
8	科云全离信单导系统	1,300.00	467.38	467.38	完成符合国军标的交换网关研制，推出若干安全接入、交换代理、互联缓冲等安全交换网关；提升影像交换单向导入设备性能至 4Mbps。	拟完成设备种类扩张，如符合国军标的交换网关研制；提升影像单向交换产品性能。	在跨网数据交换产品上处于国内领先地位，一是单向导入的设备种类最全，二是若干导入设备性能领先，三是具备交换网关能力符合相关国家和军队标准。	在大数据背景下数据共享是刚需，因此在保密行业进行安全合规的数据交换有广阔的市场前景，包括政府机关、军队军工等。
9	科云中印系统	1,500.00	448.03	448.03	完成对申威平台加统信操作系统的适配，完成新刻录打印一体机、文件自助回收柜的开发。	适配更多国产硬件和操作系统平台，完成新集中文印外设开发。	科云集中文印系统处于国内领先水平，一是入围部队国产办公项目，二是整体系统包括文印控制软件、文印交互终端、刻录打印一体机、文件自助回收柜等全套解决方案。	国际形势动荡，保密工作越发重要，如何对纸质文件、光盘等涉密载体进行全生命周期管理，是保密主管部门的强制性要求，因此在政府、军队军工有刚性需求。
10	科云数据归档	200.00	49.00	49.00	完成软 RAID、定期盘点、灾难恢复等功能，提升数据存储安全性。	提升蓝光归档系统的数据安全性。	科云数据归档系统处于国内先进水平，产品提出面向对象的数据	在大数据时代数据呈现出爆炸式增长，大量数据要求长期保存，如医疗、公检法卷宗、

序号	项目名称	预计总投资规模	本期投入金额	累计投入金额	进展或阶段性成果	拟达到目标	技术水平	具体应用前景
	系统						管理思路，对图文、音视频数据可以进行数据处理，便于快速检索。	档案数据等，蓝光归档阵列这种数据低价冷存的方式适合于长期保存数据。
合计	/	24,000.00	19,380.93	19,380.93	/	/	/	/

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

2023 年度，公司累计使用募集资金 57,198,808.47 元，收到的累计利息收入及理财产品收益扣除手续费、汇兑损益金额为 1,718,806.52 元。截至 2023 年末，公司使用闲置的募集资金用于现金管理的余额为 40,000,000.00 元，募集资金账户应有余额 3,077,472.88 元，公司募集资金账户实际余额为 3,077,472.88 元（包括累计收到的银行存款利息扣除银行手续费等的净额），与募集资金账户应有余额的差异金额 0 元。

截至 2023 年 12 月 31 日，公司募集资金使用及结余情况如下：

单位：元

项目	金额
截至 2022 年 12 月 31 日募集资金余额	55,945,474.83
减：本报告期募集资金使用金额	57,198,808.47
加：累计利息收入及理财产品收益扣除手续费、汇兑损益金额	1,718,806.52
2023 年赎回理财产品金额	42,612,000.00
减：2023 年用暂时闲置资金购买理财产品（含通知存款）金额	40,000,000.00
募集资金 2023 年 12 月 31 日应结存余额	3,077,472.88
募集资金 2023 年 12 月 31 日实际结存余额	3,077,472.88

截至 2023 年 12 月 31 日，公司募集资金存储余额情况如下：

单位：元

银行名称	银行帐号	余额
招商银行股份有限公司北京方庄支行	110935528510301	2,502,731.74
中信银行股份有限公司北京房山支行	8110701013902061324	3,133.87
华夏银行股份有限公司北京媒体村支行	10240000000565663	571,598.06
北京银行股份有限公司和平里支行	20000016706000041145161	9.21
合　　计		3,077,472.88

公司 2023 年度募集资金存放与使用情况符合《上海证券交易所科创板股票上市规则》《募集资金管理制度》等法律法规和制度文件的规定，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，募集资金具体使用情况与公司已披露情况一致，不存在变相改变募集资金用途和损害股东利益的情况，不存在违规使用募集资金的情形。

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 2023 年 12 月 31 日，公司控股股东、实际控制人李伟、王翊心、丁纯直接持有公司股票分别为 51,255,360 股、19,056,480 股、19,056,480 股，本期直接持股数因资本公积转增股本有所增加。除公司实际控制人外的其他董事、监事和高级管理人员未直接持有公司股份。

截至 2023 年 12 月 31 日，公司控股股东、实际控制人、董事、监事、高级管理人员间接持有公司股份的情况如下：

姓名	职务	投资企业名称	在投资企业享有权益的比例（%）	投资企业持有本公司股份的比例（%）	间接持有本公司的股份数（万股）
王翊心	董事、副总经理、核心技术人员	恒信世安	21.00	6.1126%	275.9904
		恒信同安	7.42	2.4142%	38.5139
		恒信庆安	8.79	1.4875%	28.1123
张庆勇	董事、核心技术人员、高级副总裁	恒信世安	10.00	6.1126%	131.4240
汪宗斌	监事会主席、核心技术人员、总工程师、信息安全研究院院长	恒信世安	1.33	6.1126%	17.4794
张蕨葆	职工代表监事、商务管理部经理、管理中心总监	恒信世安	0.67	6.1126%	8.8054
		恒信同安	2.02	2.4142%	10.4849
蒲亚梅	职工代表监事、副总裁	恒信同安	3.37	2.4142%	17.4921

注：恒信世安全称为天津恒信世安企业管理咨询合伙企业（有限合伙），恒信同安全称为北京恒信同安信息咨询合伙企业（有限合伙），恒信庆安全称为北京恒信庆安企业管理咨询合伙企业（有限合伙）。

截至 2023 年 12 月 31 日，公司控股股东、实际控制人、董事、监事和高级管理人员持有的公司股份均不存在质押、冻结及减持的情形。

十一、 上海证券交易所或保荐人认为应当发表意见的其他事项

无。

（本页无正文，为《西部证券股份有限公司关于北京信安世纪科技股份有限公司 2023 年度持续督导跟踪报告》之签章页）

保荐代表人签名：

苏华峰　　韩 星

西部证券股份有限公司

2024 年 5 月 7 日