政府采购合同书

网络与信息安全二级等保系统合同

采　购　人：贵港市中心血站

成交磋商人：广西奇异物联科技有限公司

政府采购合同书

合同编号：GGZC2021-C1-02465-GXZD

采购单位（甲方）贵港市中心血站　　采购计划号GGZC2021-C1-02465-GXZD

供 应 商（乙方）广西奇异物联科技有限公司 项目名称和编号 贵港市中心血站网络与信息安全二级等保系统建设项目 GGZC2021-C1-02465-GXZD

签 订 地 点　贵港市　　签 订 时 间 2021.9.28

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照采购文件规定条款和成交磋商人承诺，甲乙双方签订本合同。

第一条　合同标的

1、供货一览表

序号	产品名称	商标品牌	规格型号	生产厂家	数　量	单 位	单　价（元）	金　额（元）
1	上网行为管理	网神	NBM3350X	网神	1	台	95500.00	95500.00
2	漏洞扫描系统	网神	S1500-W010P	网神	1	台	116500.00	116500.00
3	堡垒机	网神	B1100-BC-5P	网神	1	台	86000.00	86000.00
4	日志审计系统	网神	LAS-R12P	网神	1	台	105000.00	105000.00
5	数据库审计系统	网神	DAS1000-TF10M	网神	1	台	111000.00	111000.00
6	终端安全管理系统	奇安信	奇安信天擎终端安全管理系统V10.0	奇安信	1	套	29700.00	29700.00
7	虚拟化安全管理系统	网神	奇安信网神统一服务器安全管理系统V8.0	网神	1	套	51000.00	51000.00
8	VPN安全网关	网神	X1500-TY14P	网神	1	台	43000.00	43000.00
9	门禁系统	中控智慧	XFACE600	中控智慧	1	套	2300.00	2300.00
人民币合计金额（大写） 人民币陆拾肆万元整　　（小写）人民币¥640000.00元								

2、合同合计金额包含：

（1）货物的价格；

（2）货物的标准附件、备品备件、专用工具的价格；

（3）运输、装卸、调试、培训、技术支持、售后服务等费用；

（4）必要的保险费用和各项税费；

（5）安装费用等所有费用。磋商报价中应包含全部内容，成交后采购人不再另行支付额外费用。如成交人因在项目实施的过程中不愿意负担该项目所有的辅材、配件，而导致项目最终无法正常运行的，采购人有权解除和成交人的合同关系，后果则由成交人自行负责。所提供的配备品备件及耗材等必须是未经使用的全新的产品。该项费用应包含在磋商报价中。如竞争性磋商采购文件对其另有规定的，从其规定。

第二条　质量保证

1、乙方所提供的货物型号、技术规格、技术参数等质量必须与竞争性磋商响应文件和承诺相一致。乙方提供的自主创新产品、节能和环保产品必须是列入政府采购清单的产品。

2、乙方所提供的货物必须是全新、未使用、未拆装过的原装产品，且在正常安装、使用和保养条件下，其使用寿命期内各项指标均达到质量要求。

第三条　权力保证

乙方应保证所提供货物在使用时不会侵犯任何第三方的专利权、商标权、工业设计权或其他权利。

乙方应按竞争性磋商采购文件规定的时间向甲方提供使用货物的有关技术资料。

没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、质押、查封等产权瑕疵。

第四条　包装和运输

1、乙方提供的货物均应按竞争性磋商响应文件要求的包装材料、包装标准、包装方式进行包装，每一包装单元内应附详细的装箱单和质量合格证。

2、货物的运输方式：陆运　。

3、乙方负责货物运输，货物运输合理损耗及计算方法：　/　。

第五条　交付和验收

1、交付时间：自签订合同之日起 30 个工作日内完成交货，交货后 10 个工作日内完成安装、

地点：贵港市港北区修正大道 2501 号　。

2、乙方提供不符合竞争性磋商响应文件和本合同规定的货物，甲方有权拒绝接受。

3、乙方应将所提供货物的装箱清单、用户手册、原厂质保卡、工具和备品备件等交付给甲方，如有缺失应及时补齐，否则视为逾期交货。

4、甲方应当在到货后七个工作日内进行验收，逾期不验收的，乙方可视同验收合格。验收合格后由甲乙双方签署货物验收单并加盖采购单位公章，甲乙双方各执一份。

5、乙方完成安装后由甲方组织相关人员进行竣工验收（自行验收），其验收时间以该项目验收方案确定的验收时间为准，验收结果以该项目验收报告结论为准。在验收过程中发现乙方有违约问题，可暂缓资金结算，待违约问题解决后，方可办理资金结算事宜。

6、甲方对验收有异议的，在验收后五个工作日内以书面形式向乙方提出，乙方应自收到甲方书面异议后 5 日内及时予以解决。

第六条　售后服务、保修期

1、乙方应按照国家有关法律法规和“三包”规定以及竞争性磋商响应文件和本合同所附的《服务承诺》，为甲方提供售后服务。

2、货物保修期：三年。

3、乙方提供的服务承诺和售后服务及保修期责任等其它具体约定事项。（见合同附件）

第七条　付款方式和保证金

1、当采购数量与实际使用数量不一致时，乙方应根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

2、资金性质：财政专户管理资金。

3、付款方式：合同签订后三十日内甲方支付合同金额的30%给乙方作为预付款，乙方提供的所有设备系统安装完毕后30个工作日内支付合同总价的55%；所有设备系统安装完毕后，并经调试、培训、验收合格正常运营后90日内支付合同总价的100%，）在每次付款前，乙方应向甲方提供正式合法有效的等额税率为13%的增值税专用发票，否则甲方有权延迟付款。

4、履约保证金：无。

第八条　质量保证金

乙方在申请最后一笔尾款时，需向甲方预留合同金额3%的质保金，乙方按合同履行质量保证义务且货物保修期满后30天内甲方无息返还。

第九条　税费

本合同执行中相关的一切税费均由乙方负担。如竞争性磋商采购文件对其另有规定的，从其规定。

第十条　质量保证及售后服务

1. 乙方应按竞争性磋商采购文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

2. 如在使用过程中发生质量问题，乙方在接到甲方通知后在24小时内到达甲方现场处理。

3. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

4.上述的货物免费保修期为 3 年，因人为因素出现的问题不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

5、无条件配合采购方做好二级等保评审的相关工作，确保采购方顺利通过二级评审。

6、在采购方延续使用本次采购的相关设备期间，持续免费为采购方提供网络安全相关的技术支持服务。

第十一条　合同的变更、终止与转让

1、除《中华人民共和国政府采购法》第50条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止。

2、乙方不得擅自转让（无进口资格的磋商人委托进口货物除外）其应履行的合同义务。

第十二条　违约责任

1、乙方所提供的货物规格、技术标准、材料等质量不合格的，应及时更换，更换不及时的按逾期交货处罚；因质量问题甲方不同意接收的或特殊情况甲方同意接收的，乙方应向甲方支付违约货款额 5%违约金并赔偿甲方经济损失。

2、乙方提供的货物如侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由乙方负责交涉并承担全部责任。

3、因包装、运输引起的货物损坏，按质量不合格处罚。

4、甲方无故延期接收货物、乙方逾期交货的，每天向对方偿付违约货款额3‰违约金，但违约金累计不得超过违约货款额5%，超过 30 天对方有权解除合同，违约方承担因此给对方造成经济损失；甲方延期付货款的，由甲方负责协调相关部门直至货款拨付为止，甲方不另行支付滞纳金。

5、乙方未按本合同和竞争性磋商响应文件中规定的服务承诺提供售后服务的，乙方应按本合同合计金额 5%向甲方支付违约金。

6、乙方提供的货物在质量保证期内，因设计、工艺或材料的缺陷和其它质量原因造成的问题，由乙方负责，费用从质量保证金中扣除，不足另补。

7、其它违约行为按违约货款额5%收取违约金并赔偿经济损失。

第十三条　验收

1. 甲方对乙方提交的货物依据竞争性磋商采购文件上的技术规格要求和国家有关质量标准进行现场初步验收，外观、说明书符合竞争性磋商采购文件技术要求的，给予签收，初步验收不合格的不予签收。货到后，甲方应当在到货（安装、调试完）后七个工作日内进行验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 乙方完成货物安装后，甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做竣工验收。

4. 竣工验收时乙方必须在现场，验收完毕后作出验收结果报告。

第十四条　货物包装、发运及运输

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

3. 乙方在货物发运手续办理完毕后二十四小时内或货到甲方四十八小时前通知甲方，以准备接货。

4. 货物在交付甲方前发生的风险均由乙方负责。

5. 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方货物已送达。

6、其他违约行为按违约货款额 5%收取违约金并赔偿经济损失。

第十五条　不可抗力事件处理

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十六条　合同争议解决

1、因货物质量问题发生争议的，应邀请国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向贵港市港北区人民法院提起诉讼。

3、诉讼期间，本合同继续履行。

第十七条　合同生效及其它

1. 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2. 合同执行中涉及采购资金和采购内容修改或补充的，经双方协商签订书面补充协议，方可作为主

合同不可分割的一部分。

3.本合同未尽事宜，遵照《合同法》有关条文执行。

4、除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止。

5、乙方不得擅自转让（无进口资格的磋商人委托进口货物除外）其应履行的合同义务。

第十八条　签订本合同依据

1、政府采购竞争性磋商采购文件；

2、乙方提供的采购响应（或应答）文件；

3、响应承诺书；

4、成交通知书。

第十九条　本合同一式陆份，具有同等法律效力，财政部门（政府采购监管部门）、采购代理机构各一份，甲乙双方各两份（可根据需要另增加）。

本合同甲乙双方签字盖章后生效，自签订之日起2个工作日内，乙方需送一份合同原件到采购代理机构，采购人或采购代理机构应当将合同副本报同级财政部门备案。

甲方（章） 2021年9月28日	乙方（章） 2021年9月28日
单位地址：贵港市港北区修正大道2501号	单位地址：中国（广西）自由贸易试验区南宁片区云英路8号五象总部大厦2号楼十一层1101、1102号
法定代表人：	法定代表人：张继洪
被授权人：	被授权人：田章海
电话：0775-4322136	电话：0771-5903626
电子邮箱：	电子邮箱：service@qiyiiot.com
开户银行：	开户银行：招商银行南宁三祺广场支行
账号：	账号：771901901410606
邮政编码：	邮政编码：
经办人： 年　月　日	

附件

广西壮族自治区政府采购项目合同验收书

根据政府采购项目（采购合同编号：　　）的约定，我单位对（　项目名称：贵港市中心血站网络与信息安全二级等保系统建设项目　）　　政府采购项目中标（或成交）磋商人（　公司名称：广西奇异物联科技有限公司　）提供的货物（或工程、服务）进行了验收，验收情况如下：

验收方式：		□自行验收		□委托验收
序号	名　称	货物型号规格、标准及配置等（或服务内容、标准）	数量	金　额
1	上网行为管理	型号：NBM3350X ★1.标准1U机架式，配置6个10/100/1000 Base-T自适应电口,2个SFP千兆光口，另有1个接口扩展插槽，内置Bypass功能模块，至少1TB硬盘容量，交流电源;提供三年硬件质保及三年URL库、应用协议库软件升级服务； ★2.适用用户数2500人,适用带宽300M,最大并发会话数16万，每秒新建连接数28，000/秒； 3.支持GRE、L2TP、WLTP、CAACWS、LWAPP、CAPWAP协议下的网络环境；系统管理，支持Web方式、命令行方式、集中管理模式； ★4.设备必须提供物理硬件bypass按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅；支持远程登录在界面实现bypass,并可进行切换； 5.应用协议库包含的应用数量不低于7100种，应用规则总数不低于30000种，URL数据不低于1.5亿条，移动应用不少于1000种； 6.可识别用户上网设备类型并作为策略条件，可将IP、IP段、VLAN作为策略条件； ★7.支持基于用户、时间、应用、源IP、目的IP和服务创建流量控制策略（在响应文件中提供该功能界面截图）； 8.日志中心支持采用企业级Oracle数据库，访问、日志中心数据必须采用https加密方式访问，避免传输过程被窃取； 9.可以基于IP、MAC、终端类型等多因素进行用户认证、识别； 10.可以为用户添加多属性，并根据用户	1	95500.00

		的属性（如职位、部门、电话、邮件等）自动进行用户分类，根据分类的结果做审计、控制策略； 11.支持对QQ账号制定策略，对聊天、登录及文件传输的行为进行记录与控制； ★12.提供对微信PC版进行行为和内容审计、记录发送/接受信息的微信账号（在响应文件中提供该功能界面截图）； 13.当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；不同网页被阻塞后会跳转不同的阻塞页面，支持用户完全自定义； ★14.支持与终端杀毒软件联动，为终端杀毒软件配置推送部署策略，并能够通过终端杀毒软件获取到PC系统信息、漏洞情况，并支持对这些信息进行准入策略设置（在响应文件中提供该功能界面截图）； 15.支持利用微信公众号进行网络接入的身份准入认证； 16. Webmail基于发件人、收件人、主题、内容、附件名、附件大小维度进行记录、告警；支持根据邮件主题、正文关键字进行阻塞并进行告警； ★17.可审计Oracle，MySql，SqlServer，PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等（在响应文件中提供该功能界面截图）； 18.所有日志可以按照用户，IP地址，匹配策略，访问控制，时间等各个列排序，可生成网页访问、论坛发帖，webmail、邮件收发、应用访问、应用流量等各种统计报表； 19.支持key免审计、key免管控、key免认证三者的灵活组合； 20.可识别私接主机个数，并可制定策略以私接主机个数为阀值进行封堵；同时可建立白名单，可生成日志； 21.可识别用户上网设备类型，“工具”对象，并可作为策略条件；可将IP段作为“地点”对象，并可作为策略条件； 22.支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志； ★23.支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗（在响应文件中提供		

		该功能界面截图）； 24.设备具备三权分立功能，减少超管权限，帮助超管免责：超管无论如何配置都无权看审计日志；审计员必须经过超管授权，审核员确认才能看日志；审核员仅能审核审计员权限是否合法，不能看日志； ★25.支持管理员账号初始密码检测，如果发现管理员未更改初始密码，能够进行提醒（在响应文件中提供该功能界面截图）。		
2	漏洞扫描系统	型号： S1500-W010P ★1.标准1U机设备，配置6个10/100/1000M自适应电口,另有2个接口扩展插槽，1TB硬盘，2个USB口，1个Console口，交流电源；提供三年漏洞特征库升级，三年硬件维修服务； ★2. Web扫描域名无限制，Web扫描任务并发数不低于5个域名；系统扫描IP地址无限制，支持扫描A类、B类、C类地址，系统扫描支持不低于50个IP地址并行扫描； 3.产品至少包含系统扫描、WEB扫描、数据库扫描、基线配置核查、弱口令扫描五大功能模块； 4.采用B/S设计架构,SSL加密方式通信，无须安装客户端，用户可通过浏览器远程管理系统； ★5.支持快速配置向导，简化配置过程，以满足快捷部署上线需求（在响应文件中提供该功能界面截图）； 6.支持自定义用户口令策略，包括密码更换周期、密码长度要求、密码复杂度要求； ★7.支持同时下发系统扫描、Web扫描、弱口令扫描任务，无需单独下发扫描任务，扫描目标可以是IP、域名、URL的任一格式（在响应文件中提供该功能界面截图）； 8.支持自定义扫描策略模板，支持按照漏洞类别、漏洞风险等级、CVE编号查看漏洞插件； 9.支持显示扫描剩余时间，随时查看扫描进度；支持实时显示扫描结果，在扫描过程中随时查看资产风险状况； ★10.支持自适应网络扫描，根据网络状况自动控制发包速率，避免影响用户网络（在响应文件中提供该功能界面截图）；	1	116500.00

		11.支持自定义立即执行、定时扫描、周期性扫描等多种扫描任务执行方式，可针对指定时间、执行对象自动执行扫描任务，并自动生成报告； 12.支持扫描通用操作系统、路由交换设备、安全设备、物联网设备、工控专用设备等； 13.支持中间件漏洞扫描，涵盖 Apache、Resin、Nginx、Tomcat、TongWeb、BIND、DOMINO 、 WebSphere 、 IIS 、 Jboss 、InforSuite 等； 14.支持主流数据库漏洞的检测，应包括但不限于：Oralce、Sybase、SQLServer、DB2、MySQL、Postgres、Informix、达梦、南大通用、人大金仓、神通等； 15.支持 SNMP 协议的漏洞检测；支持 SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP 协议的登录扫描； 16.支持指定端口扫描，限定端口扫描数量以及指定 TCP 或 UDP 端口扫描； 17.支持 Web 漏洞扫描，检测基于 OWASP Top10 标准定义扫描规则；支持自动探测指定网段中的 Web 站点，并可一键转为 Web 资产或一键下发 Web 扫描任务； ★18.支持 Web 登录扫描，包括 Cookie 认证、Form 认证、Basic 认证、NTLM 认证、Session 认证、Digest 认证等，并支持 Web 登陆验证，以确保 Web 登录成功（在响应文件中提供该功能界面截图）； 19.支持至少三种漏洞验证方式如浏览器验证、注入验证、通用验证； 20.支持通过 TELNET、SSH、SMB、RDP、WinRM 协议进行安全配置核查； ★21.产品内置标准基线核查模板，包括：等保三级检测要求、工信部配置规范、中国电信安全配置规范、中国移动安全配置规范（在响应文件中提供该功能界面截图）； 22.支持主流协议和数据库弱口令检测，支持用户自定义口令字典； 23.支持自定义导出报表模板，可定制指定漏洞等级、指定漏洞状态、指定公司信息、公司 LOGO、指定报表标题以及章节内容的报表模板，并可在导出报表时灵活选择已经定义好的报表模板； 24.产品自带诊断工具，包含 PING、WGET、		

		端口探测、Tcpdump 抓包、故障信息收集、一键诊断修复等工具。		
3	堡垒机	型号： B1100-BC-5P ★1.标准 1U 机架式，配置 6 个 10/100/1000BASE 自适应电口，交流电源，2T 硬盘存储空间；提供三年质保服务； ★2.支持 50 路图形会话或 100 路字符会话并发；配置 50 个被管资源数授权许可； 3.支持用户多次登录失败将自动锁定账户或 IP，可配置解锁时长、到期自动解锁，也可以手动解锁； 4.支持资源申请，运维场景中，对特定的资源发出工单请求，管理员审批后，可以在指定时间段内运维操作该资源； ★5.支持用户水印功能，避免数据泄露无法追责（在响应文件中提供该功能界面截图）； 6.支持基于消息等级、消息类型设置是否告警和告警方式； 7.支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云和 Ucloud 云平台的资源； 8.支持通过 Web 页面访问目标支持，包括 SSH、RDP、TELNET、VNC 和应用发布资源； 9.支持 SSH 客户端、FTP 客户端、SFTP 客户端访问目标资源；支持直接在 FTP、SFTP 客户端进行编码切换，支持 big5、GB18030 和 utf8 编码切换； 10.支持将运维资源列表导出成 xshell 和 SecureCRT 格式的配置，通过客户端快速访问资源； ★11.运维过程中支持会话协同，可邀请其他用户参与、协助操作（在响应文件中提供该功能界面截图）； 12.支持不同的用户设置不同多因子方式认证，包括手机短信和手机令牌； 13.支持用户帐号和目标设备的部门分权，不同的用户和设备可以归属于不同的部门（子部门）； ★14.支持工单权限申请，支持文件上传、文件下载、文件管理、剪切板权限的申请（在响应文件中提供该功能界面截图）； 15.支持用户的批量修改，包括重置密码、移动部门、更改角色、修改多因子配置、修改有效期、修改 IP 限制、修改 MAC 限制；	1	86000.00

		16.支持 SSH、RDP、TELNET、VNC、FTP、SFTP 协议主机，支持发布 MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client 类型的应用； 17.支持资源按标签管理，每个用户可以给每个资源打多个标签； ★18.内置常用的系统类型，包括 Linux、Windows、H3C、Huawei、Cisco，无需安装任何客户端插件，使用 H5 即可直接运维相关资源（在响应文件中提供该功能界面截图）； 19.支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量； 20.支持传统的 putty、SecureCRT、MAC Terminal 等工具,支持双人授权和多因子认证，运维资源可分页显示，并且可以根据名称、IP、标签等多种条件进行查找； 21.支持 RDP、VNC 图形操作过程中键盘输入操作记录和鼠标点击行为记录； 22.在线回放过程支持播放速度调整、拖动、暂停、停止、重新播放等播放控制操作； ★23.支持系统负载、内存信息、网卡信息、磁盘使用信息、路由表信息等运行状态信息的采集（在响应文件中提供该功能界面截图）； 24.系统内置多种系统报表和运维报表模板，支持按日、周、月为周期，自动生成报表。		
4	日志审计系统	型号： LAS-R12P ★1.标准 1U 机架式设备，配置 6 个 10/100/1000M Base-T 自适应电口，另有 2 个接口扩展插槽，1 个 Console 口，2TB 磁盘存储空间，交流电源；日志采集能力 5000EPS，日志综合处理能力 2000EPS；配置 25 个日志审计节点许可，提供三年质保服务； ★2.界面采用B/S模式,无需安装客户端，使用 IE 浏览器访问管理中心，浏览器端无需安装 Java 运行环境； 3.支持对各类网络设备、安全设备、工作站、存储设备、机房设备、其他设备、中间件、数据库、防病毒系统、服务器系统的日志、事件、告警等安全信息进行全面	1	105000.00

		的审计； ★4.支持通过 Syslog、SNMP Trap、Netflow V5、JDBC、WMI、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能（在响应文件中提供该功能界面截图）； 5.支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警； ★6.支持对资产 IP 地址（含内网 IP）的地理信息进行管理，设置单 IP 及 IP 段行政区及经纬度，支持地图显示（在响应文件中提供该功能界面截图）； 7.支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； ★8.支持日志范化策略，针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级，保证最佳范化策略匹配（在响应文件中提供该功能界面截图）； ★9.支持对日志中的源和目的 IP 地址进行自动补全，补全 IP 地址的资产、国家、区域和城市等信息（在响应文件中提供该功能界面截图）； 10.具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，可将原始信息进行自动索引，快速搜索分析各类安全事件； 11.支持对事件依据其源目的IP和端口等各类字段信息进行深入的事件追踪调查，支持无限次数的追踪调查； 12.支持以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图，且属性可增加或减少； 13.具备完善的基于规则的关联分析引擎，能够提供逻辑关联、统计关联和递归关联三种关联分析能力； 14.支持单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析； 15.支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D 地球等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报表等；		

		16.支持告警管理，告警规则可以自定义，告警可查询；支持告警归并，有效抑制重复告警，归并规则可自定义； 17.支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入； 18.提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报表，满足等保等其他合规性要求； ★19.系统支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告（在响应文件中提供该功能界面截图）； 20.支持基于角色的权限管理机制，通过角色定义支持多用户访问；支持三权分立，包括系统管理员、安全管理员、审计管理员。		
5	数据库审计系统	型号： DAS1000-TF10M ★1.标准 1U 机架式设备，配置 6 个千兆电口，2 个千兆光口，另有 1 个接口扩展插槽，1 个 Console 口，硬盘总容量 4TB，冗余交流电源；提供三年软件升级和硬件维保服务； ★2.网络吞吐量 2Gbps，SQL 审计处理能力 10000 条/秒，并发连接数 500； 3.支持液晶显示屏，提供 CPU、内存、磁盘、管理 IP 等实时展现功能； ★4.可通过端口镜像、分流器模式等旁路部署或 Agent 插件方式部署，支持通过 Agent 审计回环地址的流量（在响应文件中提供该功能界面截图）； 5.支持主流数据库：Oracle、SQL-Server、DB2 、 Informix 、 Sybase 、 MySQL 、PostgreSQL、达梦、人大金仓、南大通用、神舟通用等； ★6.全面支持后关系型数据库 Cache 的审计，包括 terminal、portal、studio、Sqlmanager、MedTrak 等工具访问的审计（在响应文件中提供该功能界面截图）； 7.支持针对 IPv6 协议的审计，支持通过 IPv6 的地址检索事件； 8.支持旁路阻断功能（非串联方式），可以对单一会话危险操作阻断，或对源 IP	1	111000.00

		操作的所有请求直接阻断； ★9.支持全文检索数据库 solr 的审计，可审计到 solr 的查询、插入行为的操作信息（在响应文件中提供该功能界面截图）； 10.支持 B/S 架构 Http 应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取 XML 返回结果； 11.支持 C/S 架构 COM、COM+、DCOM 组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人； 12.支持自动发现网络中存在的数据库，并自动添加成保护对象进行审计，简化操作，避免用户因模糊记忆引起的配置故障； 13.支持对指定时间段风险数据按不同维度进行统计排行，支持对统计数据进行下钻，获取更详细的风险数据； 14.支持审计规则针对访问工具、客户端 IP、客户端 MAC、操作系统主机名、操作系统用户名、应用账户名、数据库对象、SQL 语句执行回应等条件设置等于或不等于等条件； ★15.内置疑似 SQL 注入、跨站脚本攻击、字段猜测、代码更改等 500 种以上风险审计规则库，无需单独配置，直接调用（在响应文件中提供该功能界面截图）； 16.支持风险功能，能够以时间轴的方式将每月的风险数量以柱状图展示，并以不同颜色展示风险级别； ★17.审计检索支持全库检索、条件检索和关键字检索，检索效率达到 1 亿条数据二十秒内检索出结果，快速定位相应的审计会话内容； ★18.审计检索可根据包括时间范围、风险级别、保护对象、操作类型、客户端 IP、访问工具、数据库账户、应用账户、关键字过滤、规则名、规则组名、规则类型、客户端 MAC、客户端端口、操作系统主机名、操作系统用户名、服务端 IP、服务端端口、数据库名、返回结果、记录编号、处理状态等多种条件进行检索查询（在响应文件中提供该功能界面截图）； 19.支持检索结果自定义报表，支持 Word、PDF、xls 格式报表导出；		

		20.事件回放支持以正序/倒序方式回放，并且支持设置回放时间，针对记录前后1/2/5/30/60分钟进行回放； 21.支持自定义报表，用户可根据需求定义报表的统计内容；支持根据时间、风险级别、客户端IP、访问工具、操作类型、数据库帐号、数据库名、表名、字段名、保护对象等源信息生成报表； 22.支持用户界面告警、Syslog告警、SNMP告警、邮件告警、短信系统、短信猫等多种告警方式； 23.支持用户管理三权分立，包括审计管理员、系统管理员、安全管理员分权的用户体系； 24.管理员登陆支持静态口令认证，密码短信认证；支持密码的复杂性管理，支持限制登录时间、登录次数、锁定用户时间、超时退出时间、密码长度、密码过期时间、密码过期状态等。		
6	终端安全管理系统	**型号：奇安信天擎终端安全管理系统V10.0** ★1.控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、漏洞修复、运维管控以及各种报表和查询等功能;配置50个Windows客户端授权，4个Windows服务器授权，含3年软件升级及病毒库升级维保服务； ★2.客户端支持安装：Windows XP_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10；服务器客户端支持安装：Windows Server 2003_SP2/Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019/中标麒麟/Deepin/SUSE Linux/Red Hat Linux； 3.支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告； 4.支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件； ★5.支持linux、国产操作系统、云桌面产品等（在响应文件中提供该功能界面截图）； 6.支持远程协助终端、远程关机、重启终端；	1	29700.00

		7.支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃； ★8.对敲诈者病毒提供防护机制（在响应文件中提供该功能界面截图）； 9.支持对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页挂马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息； 10.支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置； 11.支持定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型； ★12.支持正版软件的正版序列号的读取功能，确保软件正版化（在响应文件中提供该功能界面截图）； 13.支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度； 14.支持自动发现设备的IP-MAC地址的绑定； 15.支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制；违规外联发生时支持对内外网连接状态分别设置违规处理措施； 16.支持对终端各种外设(USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限； 17.支持3项以上的主动防御技术； 18.支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力； ★19.产品具备漏洞集中修复，定时修复，自动修复；具备蓝屏修复功能（在响应文件中提供该功能界面截图）； ★20.支持与防火墙、上网行为管理联动，达到网关边界联动防御效果（在响应文件中提供该功能界面截图）； 21.支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人；邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等；		

		22.支持展示全网终端健康状态、报警信息，可方便的查看不健康、亚健康终端列表；支持展示指定时间段内指定终端修复漏洞、病毒查杀、木马查杀的情况。		
7	虚拟化安全管理系统	**型号：奇安信网神统一服务器安全管理系统 V8.0** ★1.系统支持 B/S 架构，管理员可通过浏览器登录控制中心对系统进行管理，自带高性能数据库；同时支持无代理、有代理两种部署模式，以便结合管理需求选择相应部署模式； ★2.配置 15 个虚拟终端授权许可，含终端防病毒、虚拟防火墙、入侵防御、webshel 功能模块授权，提供三年特征库升级、软件升级服务； ★3.支持 windows/linux 主流操作系统：Windows 7、Windows 10、Windows Vista；Windows Server 2003、2008、2012、2016、2019；RedHat Enterprise Linux、CentOS、Ubuntu、SUSE、中兴新支点 NewStart、BC-linux、Deepin、RE-DCOS、NeoKylin Linux 等操作系统； ★4.支持 VMware vShpere、Ctrix Xen、Microsoft Hyper-V 、Huawei Fusioncompute、H3C CAS、浪潮云等国内外主流虚拟化厂商平台，并能够采用一个管理控制中心进行统一管理（在响应文件中提供该功能界面截图）； 5.支持对终端提供分组管理、安全策略配置、安全功能防护、特征库更新、客户端程序更新等功能； 6.支持资产信息清点功能，包括服务器基础信息、进程、账户、web 站点、web 服务、端口、软件应用、数据库、启动服务、系统安装包、Jar 包、计划任务、环境变量、内核模块详细资产信息； 7.支持主动自动化病毒查杀，可支持 Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式；支持病毒查杀的结果生成报告； 8.支持快速扫描、全盘扫描；支持个性化扫描，可以提供不同路径、不同文件类型、时间等进行自定义病毒扫描查杀； ★9.支持自定义病毒黑名单、白名单功能，包含指定文件名、文件路径、文件指	1	51000.00

		纹等多种方式（在响应文件中提供该功能界面截图）； 10.提供基于“诱饵”行为监测的勒索病毒防御，Windows 平台支持针对已知勒索病毒家族及其变种，通过内存抢占模式，实现该类病毒免疫，同时保护 Windows 系统还原点，禁止还原点被恶意删除，保障系统业务恢复； 11.支持 webshell 扫描功能，支持 PHP、JSP、ASP、ASPX 等文件的恶意 webshell 检测；支持对 webshell 文件设定白名单，对文件进行加白处理，避免对网站核心系统文件造成影响； ★12.支持对主机安全缺陷、配置进行扫描评估功能，能够对 Windows 操作系统上的策略、服务、组件等进行扫描，对 linux 操作系统上的账号、服务、安全参数、进程、配置等进行扫描评估，并给出修复建议（在响应文件中提供该功能界面截图）； 13.支持 SSH、RDP、telnet 等服务的暴力破解检测，可对来自网络的暴力破解行为进行拦截，支持配置时间、破解次数、拦截时长； 14.支持主机防火墙功能，支持虚拟机/终端系统的双向控制，可提供对威胁情报实时分析网络流量功能； ★15.支持对主机进行失陷检测，并能够对失陷主机进行监控或隔离，阻止与恶意域名的连接功能（在响应文件中提供该功能界面截图）； 16.支持入侵防御功能，可针对出入虚拟机的流量进行检测识别，防御网络攻击及入侵行为；支持虚拟补丁功能，可以在 windows、linux、数据库、应用等已知漏洞修复之前，提供针对此补丁攻击的防护能力，以免遭受威胁入侵； ★17.支持对应用协议的内容进行解析和识别，包括应预置应用分类协议库，针对分类配置阻断、允许策略（在响应文件中提供该功能界面截图）； 18.支持数据中心威胁态势感知，大屏动态展示安全运维状况，结合地理位置信息全面呈现威胁攻击详情； 19.支持按总流量、入站流量、出站流量、恶意流量、新建连接维度等对流量进行统计和展示；		

		20.支持按照不同分组、虚拟机/终端、网络协议、网络协议组、国家/地区、城市，分不同威胁类别以柱状图、折线图、饼图、原始日志等形式进行展示，支持手动或者定时定期生成报表； 21.支持日志查询与操作员日志审计功能；支持 syslog 协议，可以将安全日志发送到第三方 syslog 服务器上，并支持设置特定事件进行转发； 22.产品控制中心一次授权永久有效，当虚拟化平台扩容新增时无需额外购买控制中心的扩展升级授权。		
8	VPN 安全网关	型号： X1500-TY14P ★1.标准 1U 设备，交流电源，配置 6 个 10/100/1000M 自适应电口，1 个接口扩展插槽，1TB 工业级硬盘，1 个 RJ-45 串口；配置 30 个 SSL VPN 用户授权，30 个手机令牌授权，提供三年硬件质保； ★2.整机 SSL 加密吞吐量 280Mbps，SSL 并发连接数 2 万，最大支持并发用户数 300； 3.网络接口地址配置支持 IPv6 地址，网络路由地址配置支持 IPv6 地址； 4.支持对基于 TCP、UDP、ICMP 的所有 B/S、C/S 应用系统的支持，例如视频、oa 系统、Transroute 等，无需安装插件访问 B/S 应用； 5.支持终端使用 Win7、win7 64 位、win8、win10、Mac、Linux 等操作系统登录，保证登录后能够正常访问 SSL VPN 发布的服务； 6.支持 B/S 和 C/S 的应用支持单点登录（SSO），并提供加密认证功能；访问多个应用，只须输入一次密码，支持针对不同的访问资源设定不同的SSO用户名和密码； ★7.支持对智能终端接入的网络进行控制，包含 WIFI、联通 2G/3G/4G、移动 2G/3G/4G、电信 2G/3G/4G 网络访问控制（在响应文件中提供该功能界面截图）； 8.支持自动跳转功能，用户登录后自动弹出默认的应用界面；可自定义应用图标，可自行设置智能终端应用图标、PC 端应用图标； ★9.支持与终端安全管理软件联动，可以检查终端安全软件进程，并根据是否安装	1	43000.00

		来判断用户接入情况，并能自动弹出 IE 链接提示客户下载安装（在响应文件中提供该功能界面截图）； ★10.设备支持单独对每个应用发布业务进行负载均衡，具有轮询、加权轮询、最少连接数、静态就近性、动态就近性等算法来实现（在响应文件中提供该功能界面截图）； 11.认证方式支持本地认证、USBKey、短信认证、数据库认证、邮箱认证、证书认证、动态口令认证、LDAP 认证、windows AD 认证、RADIUS 认证，并且支持本地用户名密码、证书认证、第三方证书、LDAP、短信认证、邮箱认证之间的“与”的认证；可实现 USBKey 认证、LDAP 认证、硬件特征码等多种因子绑定认证； 12.支持动态令牌 APP 根据网关配置的安全策略，实现一人一机绑定，用户账号与手机 DEVID 进行绑定，DEVID 需收集收集硬件信息经过 HASH 算法而来，达到硬件 token 的安全要求； 13.支持用户长期不登录时自动锁定，被锁定后需要管理员才能解锁； 14.管理员可分为状态管理员，系统配置管理员，VPN 管理员，应用安全管理员，防火墙管理员，IPsec 管理员，日志管理员，系统维护管理员，创建管理员可以为其分配相应的管理员权限； 15.支持应用防火墙功能，包括能够设置 URL、应用的黑白名单；能记录用户访问 Http、邮件、QQ 等信息； ★16.支持根据 IOS 或 Android 的状态 root、越狱、病毒检测状况进行准入控制（在响应文件中提供该功能界面截图）； ★17. IOS、android 客户端登陆必须支持用户名+密码+动态口令、用户名+密码+数据库认证、用户名+密码+短信认证等双因子认证方式（在响应文件中提供该功能界面截图）； 18.支持移动应用封装功能，客户上传移动应用 APP 进行封装、加固； 19.支持 iphone、ipad、android 智能手机通过 L2TP 加密通道接入网关，并访问远程服务； 20.设备可支持远程应用发布功能，发布 C/S 应用客户端界面而非整个桌面进行发		

		布。		
9	门禁系统	型号：XFACE600 1.产品类型：混合识别考勤机； 2.验证方式：人脸加指纹； 3.摄像头红外+彩色双摄像头； 4.存储容量面部容量：10000 张； 5.指纹容量：10000 枚； 6.记录容量：10 万条； 7.考勤照片数量：15000 张； 8.卡容量：10000 张； 9.采集器：ZK 光学指纹采集器。 功能参数 1.门禁功能支持简单门禁； 2.其它功能记录查询，网络报表。 其它参数 1.显示屏：5 英寸 IPS 高清屏幕； 2.键盘按键：T9 输入法； 3.通讯接口：TCP/IP； 4.其它参数可选 IC 模块/WiFi 功能纠错。 外观参数 1.产品宽度：92mm； 2.产品高度：213mm。 环境参数 1.工作温度：-15℃-45℃； 2.工作湿度:20%-80%。	1	2300.00
合　　计			9	640000
合计大写金额：　　人民币陆拾肆万元整				
实际供货日期		合同交货验收日期		
验收具体内容	（应按采购合同、采购文件、磋商响应文件及验收方案等进行验收；并核对中标或者成交磋商人在安装调试等方面是否违反合同约定或服务规范要求、提供的质量保证证明材料是否齐全、应有的配件及附件是否达到合同约定等。可附件）			
验收小组意见	验收结论性意见： 有异议的意见和说明理由： 签字：			

验收小组成员签字：
监督人员或其他相关人员签字： 或受邀机构的意见（盖章）：
中标或者成交磋商人负责人签字或盖章：　　采购人或受托机构的意见（盖章）： 广西奇异物联科技有限公司 联系电话：　　2021年9月28日　联系电话：　　2021年9月28日

关于印发广西壮族自治区政府采购项目履约验收管理办法的通知[桂财采〔2015〕22号]