合同编号 2026-067

江苏省政府采购合同

项目名称：江苏省公安厅安全保障平台通用硬件设备

项目编号：JSZC-320000-SCZX-G2025-0802

甲方：江苏省公安厅

乙方：中移系统集成有限公司

甲、乙双方根据江苏省政府采购中心江苏省公安厅安全保障平台通用硬件设备项目招标的结果，签署本合同。

一、合同内容

1.1 标的名称：公安厅安全保障平台通用硬件

1.2 标的内容：采购防火墙、入侵防御等网络安全设备（清单见附件一）

1.3 标的质量：符合采购文件需求

1.4 履行时间（期限）：自合同签订之日起的 90 个日历天内完成所有硬件设备到指定地点的供货，180 个日历天内保证质量完成所投硬件设备的安装和调试；项目整体免费质保期 7 年（自项目终验合格之日起算）。

1.5 本项目招标文件、中标供应商的投标文件，以及采购过程中有关澄清、承诺文件是本合同的有效组成部分。

二、合同金额

2.1 本合同金额为（大写）：叁佰万元整（¥ 3000000.00）人民币。

三、技术资料

3.1 乙方应按招标文件规定的时间向甲方提供货物（包含与货物相关的服务）的有关技术资料。

3.2 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。

四、知识产权

4.1 乙方应保证甲方在使用、接受本合同货物（包含与货物相关的服务）或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权和工业设计权等知

识产权的起诉。一旦出现侵权，由乙方负全部责任。

五、产权担保

5.1 乙方保证所交付的货物（包含与货物相关的服务）的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

六、履约保证金

6.1 本项目不收取履约保证金。

七、合同转包或分包

7.1 本合同范围内产品或服务，应由乙方直接供应，不得转让他人供应。

7.2 除非得到甲方的书面同意，乙方不得部分分包给他人供应。

7.3 如有转让和未经甲方同意的分包行为，甲方有权给予终止合同，并向甲方支付合同总额百分之十的违约金并退还甲方已支付的全部费用。

八、质保期

8.1 本次项目整体免费质保期 7 年（自项目终验合格之日起算）。

8.2 免费质保期内乙方应提供免费维修、更换以及软件维护升级服务，免费质保期内更换的产品和零件应均为原厂件。

九、交付期、交付方式及交付地点

9.1 交付期：自合同签订之日起的 90 个日历天内完成所有硬件设备到指定地点的供货，180 个日历天内保证质量完成所投硬件设备的安装和调试。

9.2 交付方式：根据甲方要求。

9.3 交付地点：根据甲方要求。

十、合同款项支付

由甲方按下列程序付款，每次付款前乙方需提供发票。甲方每次收到乙方发票后不迟于 30 天内完成付款。如因财政资金拨付不到位等原因，双方可协商延迟付款，甲方不承担违约责任。

10.1 预付款：签订合同后，甲方支付合同额的 30%。

10.2 进度款：乙方完成所投硬件设备的安装和调试、大数据软件的部署和调试后，甲方于 30 日内组织初验，初验合格后 30 日支付至合同额的 60%，试运行 3 个月正常，乙方提交全部报告材料，并通过甲方组织的终验，终验后 30 日内支付至合同额的 100%。

十一、税费

11.1 本合同执行中相关的一切税费均由乙方负担。

十二、质量保证及售后服务

12.1 乙方应按采购文件规定和响应文件承诺的性能、技术要求、质量标准向甲方提供产品或服务。

12.2 乙方提供的产品或服务在免费质保期内因其本身出现质量问题，根据实际情况，经双方协商，可按以下办法处理：

（1）更换：由乙方承担所发生的全部费用。

（2）合同终止处理：合同终止，并退还甲方支付的合同款，同时应承担由此产生的所有费用，甲方不承担发生的任何费用。

（3）免费质保期内，关键部件多次维修、更换的，视为产品不合格，甲方有权解除合同。乙方应退还甲方支付款项并承担由此产生的费用。

12.3 如在使用过程中发生质量问题，乙方须在接到甲方通知后的 2 小时内到达甲方现场，并解决相关问题。

12.4 在免费质保期内，乙方应对产品或服务出现的质量及安全问题负责处理解决，并承担一切费用。

12.5 合同标的对质量保证和售后服务另有要求的，按采购文件中的相关要求处理。

十三、项目验收

13.1 甲方对乙方提交的产品或服务依据采购文件上的项目需求要求、乙方响应文件及国家有关质量标准进行验收。乙方完成所投硬件设备的安装和调试、大数据软件的部署和调试后，甲方于 30 日内组织初验，通过后进入试运行阶段。正常试运行 3 个月后乙方提交全部报告材料，甲方依据采购需求要求、乙方响应文件及国家有关质量标准进行审核，通过后于 20 日内组织终验。

13.2 乙方交货前应对产品或服务作出全面检查和对验收文件进行整理，并列出清单，作为甲方验收和使用的技术条件依据，检验的结果应随服务一起提交甲方。

13.3 甲方在使用乙方提供的产品或服务前，乙方需负责培训甲方的使用操作人员，并协助甲方一起试用，直到符合技术要求，甲方才做最终验收。

13.4 对技术复杂的产品或服务，甲方可请国家认可的专业检测机构参与初步

验收及最终验收，并由其出具质量检测报告。

13.5 采购文件规定以外的验收费用由甲乙双方协商解决。

13.6 合同标的对验收另有要求的，按采购文件中的相关要求执行。

十四、合同内容的交付

14.1 乙方应保证合同标的安全运达甲方指定地点。

14.2 使用说明书、质量检验证明书一并提交甲方。

14.3 乙方在合同标的交付甲方 48 小时前通知甲方准备接收。

14.4 合同标的在交付甲方前发生的风险均由乙方负责。

14.5 合同标的在规定的交付期限内由乙方送达甲方指定的地点并经甲方验收后视为交付，乙方同时需通知甲方已送达。

14.6 合同标的对交付另有要求的，按采购文件中的相关要求执行。

十五、违约责任

15.1 甲方无正当理由拒收的，甲方向乙方偿付拒收货款总值的百分之五违约金。

15.2 因乙方原因逾期交付合同标的的，乙方应按逾期交货总额每日万分之五向甲方支付违约金，由甲方从待付合同款中扣除。逾期超过约定日期 10 个工作日不能交付的，甲方可解除本合同。乙方因逾期交付或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值 5%的违约金，并退还甲方支付费用，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

15.3 乙方所交的产品或服务不符合项目需求要求或违反乙方响应文件承诺或不符合国家有关质量标准的，甲方有权拒收，乙方应在 7 日内更换，如未按时更换，按照逾期交付处理，愿意更换但逾期交付的，按乙方逾期交付处理。乙方拒绝更换的，甲方可单方面解除合同，并由乙方赔偿由此造成的甲方全部损失。因乙方造成合同违约的外，还应支付甲方因乙方违约而支出的诉讼费、律师费、鉴定费、差旅费等合理支出。

15.4 如乙方未能履行响应文件中的承诺事项，甲方有权不再支付剩余合同款项，同时，乙方自愿放弃参加甲方后三年组织的政府采购活动，但乙方提出的理由正当，且甲方认可的除外。

15.5 乙方应按照法律法规制定安全作业规范，在项目实施过程中，乙方一方发生的一切安全事故或给第三方造成的损害，由乙方自行承担责任，甲方不对项

18.3 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合同。

十九、解决争议的方法

19.1 双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向合同签订地的南京市鼓楼区人民法院起诉。

二十、合同生效及其它

20.1 合同经双方法定代表人或授权委托代表人签字并加盖单位公章后生效。

20.2 本合同未尽事宜，遵照中华人民共和国现行法律法规有关条文执行。

20.3 本合同正本一式肆份，具有同等法律效力，甲方、乙方各执贰份。

甲方：江苏省公安厅

地址：南京市鼓楼区扬州路 1 号

法定代表人或授权代表：

联系电话：

签订日期：2016 年 6 月 24 日

乙方：中移系统集成有限公司

地址：石家庄市青园街 220 号

法定代表人或授权代表：王昀

联系电话：

签订日期：　　年　　月　　日

开户银行:招商银行股份有限公司

北京分行营业部

账号 ：8888015100002818

目实施人员负任何安全责任；若给甲方造成损失和伤害的，赔偿一切直接、间接损失。

15.6 乙未按合同规定和服务承诺提供伴随服务、售后服务的，应按合同价5%承担违约责任。

十六、廉政廉洁条款

16.1 采购过程中如发现乙方围标、串标，或向甲方行贿等违法违规行为的，一经查实，甲方有权终止合同，并不再支付乙方剩余合同款，乙方退回已支付款项，同时承诺不再参加甲方后三年组织的政府采购活动。

十七、保密条款

17.1 根据甲方项目管理要求，乙方参与项目设备采购、系统建设和服务保障过程的人员须签订保密协议，采取严格、有效的内部保密制度和措施，履行保守相关信息的义务，加强人员教育，避免无关人员获悉相关项目信息。

17.2 未经甲方同意、乙方不得以包括但不限于誊写、复印、拍照录音、录像等任何方式进行复制工程相关文件、图纸、配置信息等,建设工作产生的信息不得以任何形式泄露给非相关方。

17.3 乙方在建设过程中使用的计算机终端，存储介质等均为保密专用，不得使用其他计算机设备进行相关操作，系统调试、工程资料编写完成后所产生的文件、图纸资料等应及时交还甲方，不得私自留存。

17.4 乙方在项目执行过程中发生失泄密事件的，甲方可单方面解除合同，乙方应退还甲方已支付款项以及自付款之日起至返还之日止的中国人民银行同期贷款利息，并由乙方赔偿由此造成的甲方全部损失（包括但不限于采取补救措施所产生的费用、诉讼费、仲裁费、律师费、第三方的违约金等其他费用）。造成严重后果的，甲方将根据有关法律法规追究乙方相关责任。构成犯罪的，依法追究其刑事责任。

17.5 无论本合同是否变更、解除或终止，合同的保密条款不受其限制而继续有效，双方都应承担保密条款约定的保密责任。

十八、不可抗力事件处理

18.1 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。

18.2 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。

附件一：明细报价表

（一）硬件部分											
序号	设备名称	品牌型号	技术参数		数量	单位	单价（万元）	小计（万元）	产地	质保期	税率
1	防火墙01	奇安信网神NSG2300-FT10	*整机要求*	*CPU采用国产多核处理器芯片；*	2	台	1.5	3	北京	7年	13%
				吞吐量≥1Gbps，IPSec吞吐量≥400Mbps，最大并发连接数≥150万，SSL VPN并发用户数≥500，每秒新建数≥3万，策略数≥1.5万；							
				光模块配置：千兆单模光模块≥2个；							
				冗余电源；							
			接口规模	端口类型：固定接口≥4GE+2Combo；可扩展槽位≥2，可扩展卡类型：2×10GE（SFP+）+8×GE（RJ45），8×GE（RJ45），8×GE（SFP），4×GE（RJ45）BYPASS；							
			路由功能	支持多种路由：如静态路由、动态路由、策略路由及ISP路由等（提供设备功能截图）；							
			接入管理	支持链路聚合、虚拟线及子接口等多种网络接入方式；							
			NAT	支持源地址转换、目的地址转换、双向地址转换及端口转换功能；							
			策略管理	支持基于源地址、目的地址、应用连接限制；支持每IP连接总数限制、所有IP连接总数限制、每IP新建连接数限制；支持连接限制策略命中统计查看，显示最近被拒的地址对象节点信息，应用组对象节点信息等；							
			攻击防御检测	*基于特征检测，支持超过3500漏洞特征的攻击检测和防御，基于协议检测，支持协议自识别，基于协议异常检测，支持自定义IPS签名；*							
				系统预定义IPS签名数≥10000；							
			防病毒	引入病毒库，能够深层检测HTTP、FTP、SMTP、POP3协议，发现包括木马、后门和蠕虫在内的新近流行的多种网络病毒；							
				病毒库覆盖400万以上变种病毒；							
			质保	*配置7年IPS特征库升级许可，7年防*							

			服务	病毒功能升级许可。							
2	防火墙02	奇安信网神NSG4300-FT15	整机要求	CPU采用国产多核处理器芯片；	1	台	6	6	北京	7年	13%
				吞吐量≥30Gbps，最大并发连接数≥1100万，每秒新建连接数≥40万；							
				配置光模块：万兆多模模块≥4个，万兆单模模块≥4个；							
				冗余电源；							
			接口规模	端口类型：千兆电口≥8个，万兆光口≥8个；							
			路由功能	支持多种路由：如静态路由、动态路由、策略路由及ISP路由等（提供设备功能截图）；							
			接入管理	支持链路聚合、虚拟线及子接口等多种网络接入方式。							
			NAT	支持源地址转换、目的地址转换、双向地址转换及端口转换功能；							
			策略管理	支持基于源地址、目的地址、应用连接限制；支持每IP连接总数限制、所有IP连接总数限制、每IP新建连接数限制；支持连接限制策略命中统计查看，显示最近被拒的地址对象节点信息，应用组对象节点信息等；							
				支持一条安全策略中同时配置ipv4和ipv6地址；							
			攻击防御	能够实时阻断包括溢出攻击、WEBCGI攻击、系统漏洞攻击等网络攻击行为；具有DDOS防御、流量滥用管控、上网行为管理等功能；							
				系统预定义IPS签名数≥10000							
			攻击检测	采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段，深入分析L2-L7层网络判断入侵行为，准确的发现包括溢出攻击、RPC攻击、WEBCGI攻击、木马蠕虫传播、系统漏洞攻击等网络攻击行为；							
			应用流量监控	采用深度的识别技术，对应用协议交互过程进行智能分析，对采用动态变化服务端口或者使用标准协议端口隐藏传输内容的应用可以准确识别和控制；							
			防病毒	引入病毒库，采用基于数据流的检测技术，能够深层检测HTTP、FTP、SMTP、POP3协议，发现包括木马、后门和蠕虫在内的新近流行的多种网络病毒；							

				病毒库覆盖 400 万以上变种病毒							
			质保服务	*配置 7 年 IPS 特征库升级许可，7 年防病毒功能升级许可。*							
3	防火墙 03	奇安信网神 NSG4300-FT15	*整机要求*	*CPU 采用国产多核处理器芯片；*	2	台	4.2	8.4	北京	7 年	13%
				吞吐量≥30Gbps，最大并发连接数≥1100 万，每秒新建连接数≥40 万；							
				端口类型：千兆电口≥2 个，万兆光口≥2 个；							
				配置光模块：万兆单模光模块≥2 个；							
				过滤已知特征（如 SQL 注入等）的网络攻击，配置访问策略，仅允许访问常用端口（如 20、21、22、23、25、80、443、3389 等），同时对常用端口中的敏感端口（21、22、23、3389 等）进行认证控制，阻止一切非认证访问，并提供应用层威胁实时防护。							
			路由功能	支持多种路由：如静态路由、动态路由、策略路由及 ISP 路由等（提供设备功能截图）；							
			接入管理	支持链路聚合、虚拟线及子接口等多种网络接入方式；							
			NAT	支持源地址转换、目的地址转换、双向地址转换及端口转换功能；							
			策略管理	支持基于源地址、目的地址、应用连接限制；支持每 IP 连接总数限制、所有 IP 连接总数限制、每 IP 新建连接数限制；支持连接限制策略命中统计查看，显示最近被拒的地址对象节点信息，应用组对象节点信息等；							
				支持一条安全策略中同时配置 ipv4 和 ipv6 地址；							
			攻击防御	能够实时阻断包括溢出攻击、WEBCGI 攻击、系统漏洞攻击等网络攻击行为；具有 DDOS 防御、流量滥用管控、上网行为管理等功能；							
				系统预定义 IPS 签名数≥10000；							
			攻击检测	采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段，深入分析 L2-L7 层网络判断入侵行为，准确的发现包括溢出攻击、RPC 攻击、WEBCGI 攻击、木马蠕虫传播、系统漏洞攻击等网络攻击行为；							
			应用流量	采用深度的识别技术，对应用协议交互过程进行智能分析，对采用动态变							

			监控	化服务端口或者使用标准协议端口隐藏传输内容的应用可以准确识别和控制；							
			防病毒	引入病毒库，采用基于数据流的检测技术，能够深层检测 HTTP、FTP、SMTP、POP3 协议，发现包括木马、后门和蠕虫在内的新近流行的多种网络病毒；							
				病毒库覆盖 400 万以上变种病毒；							
			质保服务	*配置 7 年 IPS 特征库升级许可，7 年防病毒功能升级许可。*							
4	防火墙 04	奇安信网神 NSG6300-FT35	*整机要求*	*CPU 采用国产多核处理器芯片；*	1	台	5.5	5.5	北京	7 年	13%
				吞吐量≥20Gbps，IPS 吞吐量≥10Gbps，最大并发连接数≥800 万，每秒新建连接数≥20 万；							
				配置光模块：万兆多模模块≥6 个，千兆多模模块≥10 个；							
				静态动态路由功能，NAT 功能，7 层安全防护功能，攻击检测、防御功能，应用协议识别能力，病毒检测功能等。							
			接口规模	端口类型：万兆光口≥6 个，千兆光口≥4 个，千兆电口≥12 个；							
			路由功能	支持多种路由：如静态路由、动态路由、策略路由及 ISP 路由等（提供设备功能截图）；							
			接入管理	支持链路聚合、虚拟线及子接口等多种网络接入方式；							
			NAT	支持源地址转换、目的地址转换、双向地址转换及端口转换功能；							
			策略管理	支持基于源地址、目的地址、应用连接限制；支持每 IP 连接总数限制、所有 IP 连接总数限制、每 IP 新建连接数限制；支持连接限制策略命中统计查看，显示最近被拒的地址对象节点信息，应用组对象节点信息等；							
				支持一条安全策略中同时配置 ipv4 和 ipv6 地址；							
			攻击防御	能够实时阻断包括溢出攻击、WEBCGI 攻击、系统漏洞攻击等网络攻击行为；具有 DDOS 防御、流量滥用管控、上网行为管理等功能；							
				系统预定义 IPS 签名数≥10000；							
			攻击检测	采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段，深入分析 L2-L7 层网络判断入侵行为，							

				准确的发现包括溢出攻击、RPC 攻击、WEBCGI 攻击、木马蠕虫传播、系统漏洞攻击等网络攻击行为；							
			应用流量监控	采用深度的识别技术，对应用协议交互过程进行智能分析，对采用动态变化服务端口或者使用标准协议端口隐藏传输内容的应用可以准确识别和控制；							
			防病毒	引入病毒库，采用基于数据流的检测技术，能够深层检测 HTTP、FTP、SMTP、POP3 协议，发现包括木马、后门和蠕虫在内的新近流行的多种网络病毒；							
				病毒库覆盖 400 万以上变种病毒；							
			质保服务	*配置 7 年 IPS 特征库升级许可，7 年防病毒功能升级许可。*							
5	防火墙 05	奇安信网神 NSG3300-7680-F	*整机要求*	*CPU 采用国产多核处理器芯片；*	4	台	14.5	58	北京	7 年	13%
				吞吐量≥120Gbps，IPS 吞吐率≥80Gbps，并发连接≥1.5 亿；每秒新建并发连接数≥160 万；							
				配置光模块：40GE 多模光模块≥6 个，万兆多模光模块≥4 个；							
				冗余电源；							
				静态动态路由功能，NAT 功能，7 层安全防护功能，攻击检测、防御功能，应用协议识别能力，病毒检测功能等。							
			接口规模	端口类型：40GE 光口≥6 个，万兆光口≥4 个；							
			路由功能	支持多种路由：如静态路由、动态路由、策略路由及 ISP 路由等（提供设备功能截图）；							
			接入管理	支持链路聚合、虚拟线及子接口等多种网络接入方式；							
			NAT	支持源地址转换、目的地址转换、双向地址转换及端口转换功能；							
			策略管理	支持基于源地址、目的地址、应用连接限制；支持每 IP 连接总数限制、所有 IP 连接总数限制、每 IP 新建连接数限制；支持连接限制策略命中统计查看，显示最近被拒的地址对象节点信息，应用组对象节点信息等；							
				支持一条安全策略中同时配置 ipv4 和 ipv6 地址；							
			攻击防御	能够实时阻断包括溢出攻击、WEBCGI 攻击、系统漏洞攻击等网络攻击行为；							

				具有 DDOS 防御、流量滥用管控、上网行为管理等功能；							
				系统预定义 IPS 签名数≥10000							
			攻击检测	采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段，深入分析 L2-L7 层网络判断入侵行为，准确的发现包括溢出攻击、RPC 攻击、WEBCGI 攻击、木马蠕虫传播、系统漏洞攻击等网络攻击行为；							
			应用流量监控	采用深度的识别技术，对应用协议交互过程进行智能分析，对采用动态变化服务端口或者使用标准协议端口隐藏传输内容的应用可以准确识别和控制；							
			防病毒	引入病毒库，采用基于数据流的检测技术，能够深层检测 HTTP、FTP、SMTP、POP3 协议，发现包括木马、后门和蠕虫在内的新近流行的多种网络病毒；							
				病毒库覆盖 400 万以上变种病毒							
			质保服务	*配置 7 年 IPS 特征库升级许可，7 年防病毒功能升级许可。*							
6	防火墙 06	奇安信网神 NSG6300-FT35	*整机要求*	*CPU 采用国产多核处理器芯片；*	2	台	5	10	北京	7 年	13%
				网络层吞吐量≥40Gbps，IPS 吞吐率≥15Gbps，并发连接≥1200 万；每秒新建并发连接数≥40 万；							
				配置光模块：40GE 多模光模块≥2 个，万兆多模光模块≥4 个；							
				标准机架式；冗余电源；							
				静态动态路由功能，NAT 功能，7 层安全防护功能，攻击检测、防御功能，应用协议识别能力，病毒检测功能等。							
			接口规模	端口类型：40GE 光口≥2 个，万兆光口≥4 个，千兆电口≥12 个；							
			路由功能	支持多种路由：如静态路由、动态路由、策略路由及 ISP 路由等（提供设备功能截图）；							
			接入管理	支持链路聚合、虚拟线及子接口等多种网络接入方式；							
			NAT	支持源地址转换、目的地址转换、双向地址转换及端口转换功能；							
			策略管理	支持基于源地址、目的地址、应用连接限制；支持每 IP 连接总数限制、所有 IP 连接总数限制、每 IP 新建连接数限制；支持连接限制策略命中统计							

				查看，显示最近被拒的地址对象节点信息，应用组对象节点信息等；							
				支持一条安全策略中同时配置 ipv4 和 ipv6 地址；							
			攻击防御	能够实时阻断包括溢出攻击、WEBCGI 攻击、系统漏洞攻击等网络攻击行为；具有 DDOS 防御、流量滥用管控、上网行为管理等功能；							
				系统预定义 IPS 签名数≥10000							
			攻击检测	采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段，深入分析 L2-L7 层网络判断入侵行为，准确的发现包括溢出攻击、RPC 攻击、WEBCGI 攻击、木马蠕虫传播、系统漏洞攻击等网络攻击行为；							
			应用流量监控	采用深度的识别技术，对应用协议交互过程进行智能分析，对采用动态变化服务端口或者使用标准协议端口隐藏传输内容的应用可以准确识别和控制；							
			防病毒	引入病毒库，采用基于数据流的检测技术，能够深层检测 HTTP、FTP、SMTP、POP3 协议，发现包括木马、后门和蠕虫在内的新近流行的多种网络病毒；							
				病毒库覆盖 400 万以上变种病毒							
			质保服务	*配置 7 年 IPS 特征库升级许可，7 年防病毒功能升级许可。*							
7	入侵防御（含防病毒功能）	奇安信网神 P3300-3680-F	*整机要求*	*CPU 采用国产多核处理器芯片；*	8	套	11	88	北京	7 年	13%
				网络层吞吐量≥20Gbps，IPS 吞吐量≥10Gbps，并发连接数≥800 万，每秒新建并发连接数≥20 万；							
				配置光模块：万兆多模光模块≥6 个，千兆多模光模块≥6 个；							
				标准机架式；冗余电源；							
				攻击检测、防御功能，应用协议识别能力，病毒检测功能等。							
			接口规模	端口类型：万兆光口≥6 个，千兆光口≥6 个，千兆电口≥8 个；							
			攻击防御	能够实时阻断包括溢出攻击、WEBCGI 攻击、系统漏洞攻击等网络攻击行为；具有 DDOS 防御、流量滥用管控、上网行为管理等功能；							
				系统预定义 IPS 签名数≥10000							
			攻击	采用协议分析、模式识别、统计阀值							

			检测	和流量异常监视等综合技术手段，深入分析 L2-L7 层网络判断入侵行为，准确的发现包括溢出攻击、RPC 攻击、WEBCGI 攻击、木马蠕虫传播、系统漏洞攻击等网络攻击行为；							
			应用流量监控	采用深度的识别技术，对应用协议交互过程进行智能分析，对采用动态变化服务端口或者使用标准协议端口隐藏传输内容的应用可以准确识别和控制；							
			防病毒	引入病毒库，采用基于数据流的检测技术，能够深层检测 HTTP、FTP、SMTP、POP3 协议，发现包括木马、后门和蠕虫在内的新近流行的多种网络病毒；							
				病毒库覆盖 400 万以上变种病毒							
			质保服务	*配置 7 年 IPS 特征库升级许可，7 年防病毒功能升级许可。*							
8	终端数据防泄漏	安恒信息 DAS-UES-HY-XC	*功能要求*	*控制个人终端上的对外设备接口的使用，并结合深度内容识别技术监管通过其外发的数据内容；*	1	套	5	5	杭州	7 年	13%
				控制终端电脑上可安装、运行的应用软件，并对其被动/主动访问敏感数据内容的行为进行审计/阻断；							
				支持闲时增量扫描个人终端电脑上的敏感数据存储状态及终端运行的应用软件情况，并上传扫描结果至管理平台，使管理人员实时、全面的掌握内网中所有个人终端上存储的敏感数据类型、数量，发现不当存储及高危应用软件；							
			平台标准	采用 C/S 与 B/S 混合架构，支持 WEB 管理，方便运维；							
			部署方式	为满足系统高可用性，系统支持集群式或双机热备部署架构；							
			系统平台	*支持私有化部署，支持国产化芯片 ARM 等架构；*							
			适配系统	*客户端支持国产操作系统；*							
			终端标签	系统须支持基于终端设备的标签管理，可对终端标签下发策略进行管控；							
			压缩包穿透	支持识别 tar、zip、7z、win、rar 等压缩文件内容；支持压缩包穿透检测；							
			用户	服务端须支持用户信息清晰展示，用							

			管理	户姓名、邮箱、部门、组织架构、上级、用户设备、设备信息、策略信息、风险信息。并支持在平台内将用户与纳入管理的设备一键关联；							
			质保服务	*终端授权≥500；7年升级服务。*							
9	WEB应用防护	奇安信网神W3300-U080	*整机要求*	*标准机架式，多核国产CPU硬件架构；*	1	台	21.1	21.1	北京	7年	13%
				网络层吞吐率≥9Gbps，HTTP吞吐率≥8Gbps；并发连接数≥110万，最大新建连接数≥85000；防护数量根据用户合理需求配置；							
				端口类型：万兆光口≥2个，千兆电接口≥2个；							
				配置光模块：万兆多模光模块≥2个；							
				SQL注入、XSS、CSRF等WEB攻击防护功能、URL访问控制功能、防盗链功能、WEB漏洞扫描防护功能、DDOS攻击防护功能、网页防篡改功能、报表分析及告警功能。							
			功能要求	支持旁路防护模式部署，有效阻断如SQL注入攻击、网页篡改、网页挂马；							
				采用双向数据检测机制，对进出WEB服务器的HTTP/HTTPS相关内容进行深度分析；							
				针对WEB攻击内置专用特征规则库，涵盖SQL注入防护、XSS防护、爬虫防护、扫描防护、信息泄露防护、溢出防护、协议完整性检查等多种类规则；							
			防御动作	支持对触发规则行为仅告警、阻断并重定向到告警页面、添加到黑名单、添加为白名单等；							
			日志、报表和告警	提供设备管理日志、网络安全日志、网页安全日志、防篡改日志、访问控制日志、自学习策略日志等；							
				支持周期性报表输出，报表支持PDF、DOC格式							
			质保服务	*配置7年WEB应用防护特征库升级许可。*							
10	数据库审计	安恒信息DAS-DBAuditor-G1	*功能要求*	*标准机架式，采用国产多核处理器芯片；*	2	台	7	14	杭州	7年	13%
				峰值SQL吞吐量≥65000条/秒，在线会话≥20000个，在线SQL语句存储≥300亿条，支持的数据库实例数根据用户合理需求配置；							

		980-HU		*端口类型：万兆光口≥2 个，千兆电口≥2 个；*							
				配置光模块：万兆多模光模块≥2 个；							
				冗余电源；							
				基于数据资产安全访问合规，精确、全面审计，数据库安全审计日常化运营、可疑分析和安全报告，定位事件原因，支持查询、分析、过滤，实现对目标数据库系统的用户操作的监控和审计；							
			数据库兼容性	*支持商业数据库包括但不限于 Oracle、 SQLServer，开源数据库包括但不限于 Mysql，PostgreSQL，国产数据库包括但不限于人大金仓、达梦、南大通用、神通 OSCAR，行业数据库包括但不限于 Cache，非关系型的数据库包括但不限于 MongoDB，数据仓库包括但不限于 TeraDATA；*							
			数据库安全	根据解析的 SQL，对数据库服务器进行安全判断、攻击检测，面对多种攻击检测场景能有效地作出告警等处理； 能够通过审计记录发现生产数据库潜在安全威胁； 对针对数据库的 XSS 攻击行为进行审计； 对针对数据库的 SQL 注入攻击行为进行审计； 可自定义告警规则，针对所有审计结果的属性配置告警规则； 支持数据库账号登陆成功、失败的审计； 支持原始数据包留存，可通过 sftp 方式从设备中取得已记录的原始数据包；							
			SQL 操作审计	支持自定义审计界面； 支持数据采集规则定义；							
			业务关联分析	通过对浏览器与 Web 服务器、Web 服务器与数据库服务器之间所产生的 HTTP 事件、SQL 事件进行业务关联分析，定位追查访问者，包括访问者用户名、源 IP 地址、SQL 语句、业务用户 IP、业务用户主机等信息；							
			实名	支持内网主机扫描，可自动发现 IP 与							

			审计	主机对应关系； 支持导入 IP 与用户对应关系； 支持 IP 归属地审计，定位事件到 IP 所在地，并提供地图展示功能； 支持 PPPOE 等实名审计，定位审计事件到人；							
			多维度统计分析	支持自定义多维度统计分析场景，对审计结果的任意属性进行统计分析； 支持统计分析的下钻与上卷； 事件实时统计，查看统计结果时快速返回； 统计结果以饼图、柱图展示，可导出统计结果报表； 支持自定义报表，根据需求定义报表模板生成所需报表；							
			实时告警	根据审计到的网络事件，判断事件的危险级别，进行实时的响应处理，包括：Syslog 告警、SNMP Trap 告警、邮件告警，支持旁路阻断等；							
			第三方接口	支持 SNMP 方式，提供系统运行状态给第三方网管系统； 支持 Syslog 方式向外发送审计日志； 支持 SNMP Trap 方式向外发送审计日志； 支持 NTP 时间同步；							
			质保服务	*7 年原厂升级。*							
11	大数据安全审计	安恒信息 DAS-DBAuditor-G2180-HU	*功能要求*	*标准机架式，采用国产多核处理器芯片；*	2	台	8	16	杭州	7 年	13%
				不限制数据库及实例数：采用多核多平台并行操作系统，SQL 处理能力≥90000 条/秒，采用高速存储与检索技术，存储日志量≥20 亿条；							
				端口类型：万兆光口≥2 个，千兆光口≥4 个，千兆电口≥4 个；							
				配置光模块：万兆多模光模块≥2 个，千兆多模光模块≥4 个；							
				冗余电源；							
				单一设备支持包括数据审计、风险扫描、漏洞扫描、状态监控等功能；							
			数据库兼容性	*支持非关系型数据库：MongoDB、Hive、HDFS 文件系统、Hana、MPP、Hbase、ES、Solr、Redis、SSDB、Kingba；*							
			IPv6	支持 IPv6 网络配置，支持 IPv6 环境							

			支持	下的数据库协议审计；							
			敏感数据自动发现	支持自动发现hadoop大数据平台中的电话号码、身份证、社保号等敏感信息；							
			数据库服务发现	支持发现大数据集群下的各类服务和非关系型数据库并可进行智能化统计图形化展示；							
			访问行为审计	支持实时记录访问大数据平台以及NOSQL数据库的行为，提供审计日志的查询、导出功能；支持多维度统计分析；							
			审计告警	支持用户设定多等级的威胁自动告警；							
			攻击回放	支持对事件进行攻击回放。							
			日志报表	提供报表模板以及支持定制客户报表；提供日志检索接口；支持多个查询条件进行组合检索；支持全文检索、布尔检索、通配符检索；支持生成自定义统计和排名报表；							
			日志管理	支持按日志属性、日志类型、时间范围进行数据备份；支持自动与手动方式备份；支持将数据备份至其他存储上；支持还原和查询转出的日志数据；							
			质保服务	*7年原厂升级。*							
12	安全漏洞防护	安恒信息DAS-EDR-S800	*功能要求*	*包含资产盘点、端点发现、多级管理、虚拟化管理、杀毒管理、威胁详情、勒索防护、漏洞管理、进程管理、账户风险、主机资产管理、能耗管理、主机防火墙、入侵防御模块*	1	套	5	5	杭州	7年	13%
			平台标准	*提供B/S架构集中管控平台，提供图形化安装界面；*							
			部署模式	采用客户端-服务端架构，服务端支持级联模式以满足大规模跨地域部署需求；							
				客户端支持离线模式部署，而非功能精简化的单机版，可生成相应离线安装包；							
				支持客户端远程卸载；							
			系统兼容	服务端支持国产化版本操作系统；							
				客户端支持多类型操作系统，包括							

			性	Windows Server 2008/2012/2016/2019，Windows XP SP3/vista/7/8/10/11；Ubuntu 16.04.6 LTS/18.04.6 LTS，麒麟以及 UOS 国产化操作系统；								
				支持 VMware、华为 FusionSphere、华三 CAS、品高云、Citrix Xen Server 、微软 Hyper-v 等；								
			入侵侦测和防御	支持实体、虚拟及云端运算的服务器防御；								
				支持防堵在应用程序和操作系统上已知及未知的漏洞；								
				支持防止网页应用程序遭到 SQL injection 及 Cross-site 跨网站程序代码改写的攻击；								
				阻挡针对业务系统的攻击；辨识可疑活动及行为，提供主动和预防措施；								
				提供数据库、网页、电子邮件和 FTP 服务器等不少于 100 个应用程序的漏洞保护；								
			完整监控	监视关键操作系统和应用程序，如目录、Registry keys 及数值，以侦测出恶意和不寻常的更改；								
				提供灵活且实用的监控，提供包含/排除和可审核报告；								
			应用程序管理	支持应用程序控管规则，增加对应用程序访问网络的控管及可见度；								
			日志审查	收集和分析操作系统和应用程序日志中的安全事件； 可侦测可疑行为、收集数据中心的安全事件和管理操作，并创建进阶规则；								
			反病毒引擎	适用各种终端系统及网络环境下的病毒查杀，提供多引擎杀毒能力；								
				支持国产桌面终端的病毒查杀，至少包括云查杀引擎、大数据特征引擎、人工智能引擎、脚本引擎等，支持针对信创终端 ELF 文件的病毒查杀，客户端支持以图形化方式展示引擎信息；								
			扫描策略	发现病毒时支持由客户端用户选择仅扫描或由系统自动处理。支持实时防护开关；支持实时防护文件大小设置；支持防护等级设置；支持压缩包防护								

				设置；支持勒索软件等恶意软件行为进行监控检测及防护；							
				支持自定义扫描程序 CPU 使用率、内存占用大小阈值；							
			漏洞扫描	支持设置指定的时间自动扫描漏洞，可设置多个不同的时间。支持排除漏洞，建立排除漏洞列表；							
			补丁管理	补丁生效管理：补丁安装完成后提示重启/自动重启（使补丁及时生效），支持不少于 3 种重启策略设置方式；							
			漏洞管理	支持对扫描出的操作系统漏洞、第三方组件漏洞能执行一键修复或者进行关联规则设置，解决系统应用层面高危漏洞利用问题；							
			控制策略	记录资产详情，包括：ID、名称、状态、镜像、创建时间、宿主节点、宿主 IP、上次查杀病毒、上次查杀时间等；							
			弱口令检测	支持系统/应用弱口令定时扫描任务、支持设置弱口令检测白名单；							
			账户使用审计	支持账户使用监控，监控账户登录、新增、删除、注销、修改密码等行为，同时针对账户更改信息也可做相关审计，包含：更改账户全名、所属组、权限信息、更改“用户下次登录时需更改密码”、更改“用户不能修改密码”、更改“密码永不过期”、更改”用户已被禁用“设置、更改”账户已锁定“设置等；							
			策略设置	支持配置前置条件和检查条件，支持根据应用场景自行配置，终端根据管理员定义的配置和内容，自动完成检查；支持用户自定义安全体检项；							
			质保服务	*服务器操作系统防护授权≥200；7 年升级。*							
小计								240			

（二）服务部分

序号	服务内容	数量	单位	单价（万元）	小计（万元）	税率

1	集成服务	1	年	60	60	6%
投标报价总计	¥3000000 元	人民币（大写）：	叁佰万元整