开封公安网络安全体系建设项目合同

甲方：开封市公安局

乙方：郑州云智信安安全技术有限公司

签约地点：开封市公安局

签约时间:2025 年 4 月 1 日

甲乙双方根据 2025 年 03 月 26 日开封市公共资源交易中心有限公司签发的开封市公安局采购开封市公安局公安网络安全体系建设项目中标通知书和招、投标文件及其它有关文件内容，经双方协商一致，达成以下合同条款：

一、本合同所指设备（工程）详见附件一设备清单（附后），合同总价款为人民币￥2,726,859.00 元（大写：贰佰柒拾贰万陆仟捌佰伍拾玖元整）。

二、设备（工程）质量要求及乙方对质量负责的条件和期限：

乙方提供全新设备（包括零部件、附件、备件备品），设备必须符合国家标准或行业标准要求，行业标准高于国家标准以行业标准为准，且应达到招投标文件及澄清中的技术标准。进口设备具有原产地证明、生产国质量证明及国家进口商检证明。

甲方对设备有异议的应在收货 3 日内以书面形式向乙方提出。

售后服务要求按照招标文件及投标文件的相应条款执行。即：自系统通过验收之日起，乙方对系统实行五年免费保修，网络安全运维驻场服务 4 年；在系统出现故障时，乙方接到甲方报修电话后应在 2 小时内到达现场解决，并在 8 小时之内修复，解决不了的故障应在 12 小时内免费提供同型号的替代产品进行更换,保证系统正常运行，每超过 12 小时没有修复故障的每次承担合同标的额的 3%作为违约金。功能增减和功能升级免费实施，同时免费提供与其它系统信息交换的接口。

我公司提供 7*24 小时的技术咨询服务和故障服务受理，同时配置 2 名现场驻场人员，如遇重大突发事件（如自然灾害、人为因素造成系统大面积故障等）或特殊时期（如系统软件全面升级、上级检查、执行重大任务等）提供的服务计划及承诺（如果设备出现故障，更换备机服务时限）。

三、合同履行的地点及工程进度：合同生效后，乙方应于合同签订日

起30个日历天内按甲方要求在甲方指定地点完成设备的安装调试。设备运送产生的费用由乙方负责。甲方应在设备到达指定地点后，提供符合安装条件的场地、电源、环境等。

四、乙方在交付设备时应向甲方提供设备的使用说明书、合格证书及其它相关材料。

五、乙方在施工过程中应确保施工安全，如发生安全事故，由乙方承担全部法律责任。

六、为实现系统功能未列出的设备、软件及附件耗材等，乙方应自行承担。

七、验收：乙方在所有设备完成供货施工完毕后，甲方组织验收、审计。

八、乙方须免费提供一次项目涉及的软件、设备和系统的迁移，保证甲方正常使用。

九、人员培训：乙方按招标文件规定和甲方要求对甲方人员进行技术培训。

十、付款方式及期限：

1.签订合同后乙方支付甲方3%的履约保证金，保证金为保函形式，在验收合格且无违约行为时将履约保函退回。

2.签订合同后，货物（设备）到达采购人指定位置支付合同价款的30%，项目完成最终验收经审计后，按审计结果支付剩余价款。

十一、违约责任：

1、乙方未按期交付设备（工程）的，每超过1日应由乙方支付合同标的额3‰的违约金，甲方同时有权要求赔偿损失。超过20日乙方不能交付设备的甲方有权解除合同，乙方应向甲方支付合同标的额30%违约金，并赔偿因此给甲方造成的损失。

2、所交的设备品种、规格、型号、质量等不符合合同规定标准的，甲方有权拒收设备，解除合同，乙方向甲方支付合同标的额30%的违约金。

3、甲方无正当理由拒收设备，应向乙方偿付拒收设备款额5%的违约金。

十二、甲乙双方应严格遵守本合同及招投标文件要求，如有违反，按本合同约定予以处理。

十三、因设备的质量问题发生争议，由法定的技术鉴定单位进行质量鉴定。

十四、招标文件及其修改、投标文件及其修改、澄清、变更单、审计报告均为本合同的组成部分。

合同组成部分效力优先级为：审计报告、本合同、变更单、招标文件及其修改、投标文件及其修改、澄清。

十五、本合同的签定和履行适用中华人民共和国法律，因履行合同发生的争议，由甲乙双方直接协商解决，如协商不成可向开封仲裁委员会仲裁解决。仲裁裁决对双方均有约束力。

本合同约定的联系方式作为双方往来沟通信函地址和发生争议无法协商解决时作为争议处理机关送达法律文书地址，如有变更应五日内书面告知对方，否则承担因此引起的法律责任。信函被退回之日视为送达之日。

十六、合同生效及其它：

本合同经双方合同代表签字盖章后生效。本合同一式六份，甲乙双方各持三份。

（以下无正文）

甲方（盖章）：开封市公安局

地址：开封市九大街与安顺路交叉口东北角

委托代理人：

电话：0371-25958899

开户行：农行开封市金明支行

帐号：16100101040029774000000037

乙方（盖章）：郑州云智信安安全技术有限公司

地址：河南省郑州市高新技术产业开发区河阳路 186 号 9 号楼

委托代理人：张晓

电话：0371-55906595

开户行：中国光大银行股份有限公司郑州淮河路支行

账号：52100188000045631

合同条款

1．定义

1.1＂甲方＂系指接受合同货物及服务的企业或单位。此次的甲方：开封市公安局；

1.2＂乙方＂系指提供合同货物和服务的企业或单位。此次的乙方为：郑州云智信安安全技术有限公司；

1.3＂合同＂系指甲方和乙方(以下简称合同双方)已达成的协议，即由双方签订的合同格式中的文件，包括所有附件等组成合同部分的所有其他文件。

1.4＂合同价格＂系指根据合同规定，在乙方全面正确地履行合同义务时需甲方应支付给乙方的款项。

1.5＂货物＂系指乙方按合同要求，须向甲方提供的设备、软件、工具、备品备件、手册以及其它有关技术资料和材料。

1.6＂服务＂系指合同规定乙方须承担的运输、安装调试、技术协助、人员培训、技术服务、售后服务和其它类似的义务。

1.7“交货地点”系指将要进行货物安装和运转的地点。

2．适用范围

2.1本合同条款适用于开封市公安局公安网络安全体系建设项目。

3．原产地

3.1原产地系指货物的生产地，或提供辅助服务的来源地。

4．技术规格和标准

4.1本合同项下所供货物的技术规格应与方案所陈述技术规格规定的标准相一致或优于。

5．专利权

5.1乙方须保障甲方在中国使用其货物、服务及其任何部分不受到第三方关于侵犯专利权、商标权、工业设计权、和软件著作权的指控。任何第三方如果提出侵权指控，乙方须与第三方交涉并承担由此而引起的一切法律责任和费用。

6、包装

6.1 除非本合同另有规定，乙方提供全部货物，均应采用标准保护措施进行包装。

7、交货时间、地点和方式

7.1 交货时间：签订合同后 30 日历天内完成供货安装。

7.2 交货地点：乙方负责办理运输和保险，将货物运抵甲方指定的交货地点。有关运输和保险的一切费用由乙方承担。所有货物到达甲方指定地点并经甲方验收确认日期为交货日期。该日期迟于 7.1 项约定的，为延期交付。迟延交付应承担相应责任。

8、价格和支付

8.1 本合同计价单位为人民币“元”。

本合同总价格为人民币￥2,726,859.00 元（大写：贰佰柒拾贰万陆仟捌佰伍拾玖元整）

8.2 付款比例及付款时间按照合同执行。

9、技术资料

9.1 乙方向甲方提供合同设备相符的中文技术资料，随货物包装提供给甲方。如本条款所述资料寄送不完整或资料丢失，乙方应在收到甲方通知后立即免费另寄。

10、质量保证

10.1 乙方应保证其提供的货物是全新的、未使用过的，并在各个方面符合合同规定的质量、规格和性能要求。在规定的质量保证期内，乙方应对由于设计、工艺或材料的缺陷而造成的任何缺陷或故障负责。

10.2 合同项下系统的质量保证期为：验收合格后五年保修服务。

11、安装及服务

11.1 系统安装及培训在合同条款中有明确规定；

11.2 保修期内服务：

a. 服务范畴：提供自所供系统安装调试开通之日起

I. 保修期内的现场维修服务，所产生的一切费用由乙方负责。

II. 五年免费备件供应，包括相关零部件。

III. 五年免费备件供应期满后，提供二年备件供甲方采购。

b.保修期限：本项目验收合格之日起，免费保修 60 个月。

11．3 保修期外服务：

a．保修期外单次付费维修

b．续保服务

内容与保内服务相同

12、延期交货/付款

以合同为准。

13、不可抗力

13．1 签约双方任一方由于受诸如战争、严重火灾、洪水、台风、地震、国家政策等不可抗力事故的影响而不能执行合同时，履行合同的期限应予以延长，则延长的期限应相当于事故所影响的时间。不可抗力事故系指供需双方在缔结合同时所不能预见的，并且它的发生及其后果是无法避免和无法克服的事故。

13．2 受阻一方应在不可抗力事故发生后尽快用电报或传真通知对方，并于事故发生后 7 个日历天内将有关当局出具的证明文件用特快专递或挂号信寄给对方审阅确认。一旦不可抗力事故的影响持续 60 日历天以上，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14．税费

14．1 所有应交纳的一切税费均由乙方承担。

15．争议解决方式

15．1 在执行本合同中发生的或与本合同有关的争端，双方应通过友好协商解决，经协商不能达成协议时，交由合同签订地开封仲裁委员会仲裁解决。

16．因违约之解除合同

16．1 如果乙方未能在合同规定的期限内或甲方准许的任何延期内交付部分或全部货物，或甲方未能在合同规定的期限内或乙方准许的任何延期内付款；

16．2 乙方 / 甲方未能履行合同项下的任何其它义务包括：

乙方不能供货或供货逾期 20 天以上。

17．合同修改

17．1 欲对合同条款作出任何改动，均须由供需双方签署书面的合同修改书。

18．转让与分包

18．1 本项目乙方不得转让和分包，否则甲方不予付款。

19．适用法律

19．1 本合同应按中华人民共和国的法律解释。

20．通知

20．1 双方可以用任何通讯手段交换意见和信息，但非双方盖章书面确认的，均不发生法律效力。

甲方地址：开封市九大街与安顺路交叉口东北角

甲方电话：0371-25958899

乙方地址：河南省郑州市高新技术产业开发区河阳路 186 号 9 号楼

乙方电话：0371-55906595

21．合同生效及其他

合同未尽事宜，双方协商补充，补充协议与本合同具备同等法律效力。

（以下签署页，无正文）

甲方（盖章）：开封市公安局

地址：开封市九大街与安顺路交叉口东北角

委托代理人：

电话：0371-25958899

开户行：农行开封市金明支行

帐号：16100101040029774000000037

乙方（盖章）：郑州云智信安安全技术有限公司

地址：河南省郑州市高新技术产业开发区河阳路 186 号 9 号楼

委托代理人：张晓

电话：0371-55906595

开户行：中国光大银行股份有限公司郑州淮河路支行

账号：52100188000045631

附件一设备清单

序号	产品名称	规格型号	品牌	产品具体描述	数量	单位	单价（元）	合价（元）	备注
1	公安信息网“一机两用”监控系统侦听器系统V6.0	万兆硬件	北信源	**硬件性能指标：** 1、2U一体化硬件设备； 2、1个1000BASE-T管理口，1个Console口，1个双机热备接口，2个USB口，4个1000BASE-T电口，2个万兆光口，可支持扩展到4个万兆光口； 3、最大吞吐量10Gbps； **功能指标：** 1、具备2路业务接入，可支持到4路业务接入； 2、具备与本单位“联网平台”监控系统对接能力，自动同步本地的注册资产信息，保护资产信息、阻断资产信息。 3、具备与公安部“联网平台”一级总控制对接能力，实现本地发现的灰名单资产上报和接收一级总控下发的全国黑名单资产。 4、具备对黑名单资产的阻断能力。 5、设备支持高可用，双机热备能力。可满足公安信息网安全运维考核要求。（提供完整考核要求文档） 6、数据高可用，具备黑名单资产数据定时同步能力。 7、具备资产指纹分析能力，对发现的联网设备进行详细信息识别 8、具备对识别到的设备信息可同步到“联网平台”资产列表。（提供接口证明文件） 9、具备对未处置设备的发现和自动阻断功能。	2	台	212,500	425,000	“一机两用”侦听器
2	“一机两用”监控及设备资源管理系统(国产操作系统版)V6.8		北信源	**升级改造内容：** 1、适配当前市局配发的国产化终端主机，满足国产终端主机“一机两用”软件的安装，对接入公安网的国产化主机进行相应的审计、管控等； 2、“一机两用”系统管理平台三套集群组件部署工作； 3、基于用户现场已经配发的各种类型国产化终端，进行“一机两用”V9200增强版软件安装前的安装适配性测试工作，根据测试结果，对可能产生的安装故障风险进行避险处置，包括提供必要的软件改造、硬件终端的安装适配、软件功能测试、监控能力测试等，确保同批次国产化终端主机“一机两用”软件	1500	套	450	675,000	“一机两用”平台技术服务及终端授权

				的顺利安装； 4、根据对各种类型硬件终端的安装测试情况，进行各种类型终端主机增强版软件的压缩、封装、上传、下载以及同步更新相应安装手册，提供必要的安装辅助等； 5、针对公安系统已经配发、即将采购、预期升级的各种类型国产化终端主机环境，提供服务期内高质量的“一机两用”V9200 增强版软件的同步升级、改造、适配及相关的服务支撑工作，本期支持 1500 台终端； 6、升级原有 Windows 客户端，满足新的业务架构下，对原有 Windows 终端主机的接入及安全审计、管控； 7、升级原有 Linux(CentOS 和 Redhat)客户端，满足新的业务架构下，对 Linux 终端主机的接入及安全审计、管控； 8、提供二级管理集群平台的注册接入、策略同步更新、数据上传等，依据公安部相关安全管理规定进行实名化管理，便于违规外联、网络安全事件发生时快速定位到事件源 9、“一机两用”V9200 增强版软件功能内容： （1）基础功能：针对接入公安网终端进行违规外联监测、网关准入及许可接入、载入等方面的策略管理； （2）终端安全加固功能：针对接入公安网各类型终端，实现对终端无线连接方式、点对点协议、动态主机协议、网络协议代理等协议层的安全加固； （3）安全管理功能：针对接公安网主机进行终端文件系统、杀软配置、屏幕保护、IE 设置、痕迹、邮件等涉及重要安全保障的节点进行策略管理。 **技术服务内容：** 1、提供每月一次的现场巡检服务，重点检查系统运行情况，切实提升一机两用监控系统正常运行率； 2、根据市局公安网的实际使用情况，对其系统安全策略进行合理的修改； 3、根据公安部要求或策略要求，对市级系统进行同步升级，并维护升级期间的系统稳定接入，并说明升级有关的具体事宜； 4、检查系统服务器的安全状况，包括相关资源的占用情况，系统自身补丁更新情况，以及对系统进行病毒检查； 5、根据系统服务器报警信息，配合管理员处理内网中主要存在的问题； 6、对一机两用安全管理员进行的产品使用、安全管控、信息上报、突发任务调度等工作的培训和辅助开展；					

				7、对系统产生的数据进行备份并整理。对服务器端的数据库及相关审计日志进行备份，并对原有无用数据进行清理，以保证服务器运行的稳定性和安全性。提供数据备份服务； 8、提供巡检的汇总报告，存档及向主管安全领导汇报； 9、提供对一机两用正常运行率、一机两用注册率、防病毒软件覆盖率等公安部考核进行技术支持； 10、一机两用系统厂商在接到故障报告后，根据相应的事件级别，进行相应级别的应急事件响应及处置； 11、针对重大活动安保需要或敏感、特殊时期，提供终端安全保障服务，协助安全管理员做好终端安全的技术保障工作，确保相关活动、会议的顺利进行。					
3	远望主机监控与审计系统 V4.1		远望信息	**产品功能：** 1、支持网络状态监测功能，系统的网络状态监测组件实时监测计算机的网络状态变化情况，第一时间发现其网络结构特性变化后启动违规外联分析，如发现违规外联则第一时间调用通信防火墙阻断该计算机的网络通信，确保公安信息网信息安全； 2、支持实时抓包分析功能，系统可实时抓包分析组件在计算机存在网络通信的情况下，实时监测其所有网络通信数据包，发现存在非公安信息网范围内的网络通信数据包，实时启动违规外联分析； 3、支持 IP 都中名单控制功能，系统可通过自动学习方式构建 IP 控制白名单，只允许终端主机与白名单库公安信息网 IP 地址范围通信，所有超出该白名单地址范围的通信都会被阻止，通过此方式可以彻底限制终端主机可用的网络范围； 4、支持定时外联监测功能，系统可定时外联监测是传统的“一机两用”监测方式，在违规外联管控方案中也结合了此种方式，以一定的时间频率探测计算机的违规外联行为，如发现可疑行为，即刻启动违规外联分析； 5、支持离线断网控制功能，系统可监测公安信息网计算机联网状态，公安网计算机一旦脱离公安网，则禁止其网卡所有网络数据通信，使公安网计算机形成离网单机，阻断连接任何公安网以外的网络，避免发生违规外联。 6、支持违规外联告警接收功能，系统客户端可感知应用层的请求-应答回路（公安信息网与互联网），从而发现“内外网互联”通道，客户端一旦感知到互联通信链路（包括 IPV4 和 IPV6），会向此链路发送验证数据包，数据包能到达外网监测服务器，即表明互联违规行为的存在。	1	套	330,000	330,000	“一机两用”系统加固和处置

				7、支持内外网设备混用告警接收功能，客户端向浏览器以静默的方式推送和运行插件，用户使用浏览器时触发插件检查网络环境，并将取到的信息缓存在本地，具备条件时向外网服务器发送或再次回到内网时向内网服务器发送。 8、支持线路外联告警接收功能，系统客户端通过收集内网所有的非公安网地址，发现后向外网监测服务器发送探测包，如果探测包可以和外网监测服务器通信，则表明公安网内存在线路外联情况； 9、支持告警详细情况记录功能，系统可对告警发生的具体时间、告警的 IP 地址、MAC 地址、部门、联系电话、互联网出口地址、互联网出口端口号、互联网 IP 归属地进行详细的记录和留存，方便事后的原因分析和回溯； 10、支持告警及时通知功能，系统可第一时间对发现的违规外联行为进行通知提醒，可通过邮件、短信方式告知管理人员。 11、支持建立信息发布、工作成果展示的统一安全门户，需满足安全信息类、通知公告类、安全考核类、安全事件类、安全目标、应急预案、安全服务等信息的发布、维护、管理。 12、支持登录后能够查看网络内详细资产、风险、运行、业务、处理、考核等信息，落实“监测、警示、处置、反馈、考核”五位一体的管理模式，实现安全管理工作的信息化、网络化。 13、支持安管组织信息展示，在安全门户宣传和展示包含组织机构和人员的安全主体信息； 14、支持安管组织信息展示，在安全门户宣传和展示包含组织机构和人员的安全主体信息； 15、支持应急预案信息展示，安全管理工作中对于重要的安全隐患预先设定的响应处置方案； 16、支持多种业务流程类型应包含通知、签到、巡检、申报、通报、预警等，满足不同场景业务处理需求； 17、支持能够联动各级安全管理人员协同处理安全事件或异常告警，协助落实安全职责； 18、支持多种业务处理方式，应包括签收、反馈、审核、审批、打回等，能够与实际工作场景匹配； 19、支持流程自定义，能够根据实际业务自定义流程，满足各类安全业务需求； 20、支持流程管理，包含流程信息的查询、发起和处理； 21、支持流程模板配置：流程模板信息的查询、添加、修改和删除；					

				22、支持内容模板配置：内容模板信息的查询、添加、修改和删除； 23、支持回执模板配置：回执模板信息的查询、添加、修改和删除。					
4	银河麒麟桌面操作系统V10		麒麟软件	**产品功能：** 能够满足公安局工作的特殊性，可支持安装公安部三所的公安专用数字证书插件，支持并提供针对证书的系统适配，可配合用户在私有化商店在线推送安装包，即对现有操作系统进行补丁包升级服务，在线自动安装证书驱动推送公安数字证书驱动客户端，升级后系统即可实现相关功能。满足后期市直及区县可在采购前告知公安专用即可提前预装，无需二次升级。	1500	套	120	180,000	数字证书升级授权
5	公安数字证书	GUGH-20	辰锐	**产品功能：** 支持国密版算法，可兼容国产化终端和非国产化终端。	1000	个	120	120,000	加密版数字证书介质
6	猎鹰终端安全管理系统V9.0		猎鹰安全	1、提供产品授权许可包含1个系统中心+100个服务器客户端+6000个客户端。 2、系统具有网络版病毒实时查杀，终端统一管理以及日志报表等功能，猎鹰终端安全管理系统V9.0具有防病毒、漏洞管理、边界管理、软件管理、网络管控、XP防护盾、单点维护、流量管控、U盘禁用或查杀等模块，三年升级服务。 3、系统具备病毒防御、查杀支持未知病毒增强检测，支持一键云查杀、全盘查杀、指定位置查杀、U盘查杀、宏病毒专杀等； 4、系统具备漏洞管理功能，支持全网查看、修复终端漏洞，制定漏洞修复计划任务； 5、系统具备边界管理功能，支持对通过边界（U盘、互联网、下载工具、通讯软件）进入终端系统文件进行防御查杀、鉴定分析； 6、系统具备软件管理功能，支持全网软件安装统计、软件禁用、软件分发； 7、系统具备网络管控功能，支持通过网络地址、通讯方向、端口等限制终端访问权限； 8、系统具备XP防护盾功能，对XP客户端提供特有安全防护，应对微软停止更新后的安全风险； 9、系统具备单点维护功能，支持预览终端的账号、服务、网络、软硬件资产、进程、漏洞等信息，提供文件分发、消息通知、远程关机等运维功能； 10、系统具备流量管控功能，支持对终端上行、下行流量进行管控； 11、系统支持U盘等移动设备接入电脑自动检测功能，支持允许或禁止终端使用USB存储设备，如U盘、移动硬盘等；能够全面拦截和清除U盘等移动设备	1	套	260,000	260,000	终端安全系统

				可能带来的病毒木马。					
7	瑞星防毒墙 RSW5.0	RSW-NL8980	瑞星	1、支持对双归属链路环境的支持，可以满足非对称路由网络环境的需求； 2、支持双归属链路中的不同链路的两台墙之间的 URL 数据同步功能； 3、支持非代理应用层杀毒技术，保证不改变经过防毒墙数据的任何特征，做到“透明代理”更加透明； 4、支持对网络中半连接的数据进行病毒查杀功能； 5、支持日志功能、可提供病毒日志、隔离日志、管理日志等。	1	台	236,859	236,859	防毒墙
8	网御运维安全网关 LA-OS/V3.0	LA-OS-6600-S	网御星云	1、可管理设备数：200 个 IP 授权； 2、硬盘容量：内置存储 1T 硬盘； 3、运行性能并发数：600 个字符并发，100 个图形并发；支持双机热备和集群部署，支持系统配置以及审计日志实时同步； 4、支持日志存储超过设置的阀值进行邮告警，支持定期删除计划； 5、支持通过 FTP 和 SFTP 进行系统配置和审计日志备份。 6、支持导出日志可以使用离线播放器； 支持管理协议类型： 7、图形终端协议：RDP、WinRDP、VNC、X11； 8、支持字符终端协议：Telnet、SSH；文件传输协议：FTP、SFTP； 9、支持的数据库类型：Oracle：PLSQL、TOAD、SQLPLUS、SQLDEVELOPER、Mysql：MYSQLFRONT、HIDESQL、Sqlserver：SQLserver（2000-2012）； 10、支持的 WEB 类型：HTTP、HTTPS； 11、支持的其它应用：REALVNC。	1	台	100,000	100,000	堡垒机（核心产品）
9	网络安全运维驻场服务	/		1、提供针对项目建设的相关工作，确保做好项目架构整体规划、设计、部署、安装和调试,组织安装调试一机两用，确保信创电脑终端的一机两用和数字证书客户端适配、可用。 2、提供专职驻场运维人员，负责一机两用的日常系统运维，按照局方要求，完成上级对注册率、系统运行率、清理待处置设备、监控黑名单、杀毒软件安装率、系统安全加固率以及违规外联监控等方面的运行维护考核要求。根据公安部工作要求技术升级一机两用系统及一机两用客户端软件。 3、提供专职安全技术服务人员，确保做好日常网络防御。同时在上级或市局开展的网络攻防演练中，负责防御本级网络和数据安全，对市局开展网络攻防演练提供支持和配合，定期开展对网络攻防知识和技术的培训。	4	年	100,000	400,000	无

				4、提供针对全网安全设备进行管理维护，监控安全设备的运行状态、流量信息、告警信息，及时处置各类安全事件，并协助对设备进行维护、升级等。 5、结合业务系统安全防护需求，对安全设备防护策略进行调整和持续优化。 6、提供重要系统服务器、网络设备、安全设备等进行漏洞扫描、分析，提交分析报告、安全加固建议。 7、在局方指挥下定期发布安全漏洞通告、病毒预警通告和行业安全事件通告，重大安全事件即时通告。 8、项目运维服务期内为本次项目提供1名网络安全工作运维人员服务，该名服务人员满足招标文件所列的所有相关的技术能力要求，并具有行业内2年以上工作经验。					
其他费用			无							
金额总合计			大写：贰佰柒拾贰万陆仟捌佰伍拾玖元整，小写：¥2,726,859元							