|  |
| --- |
|  |
| 竞价文件 |
|  |
| \* \* 竞价前请认真阅读本文件 \* \* |
| 项目名称：纳雍县人民医院网络安全设备及维保服务采购采 购 人：纳雍县人民医院项目预算：408,886.00元采购平台：贵州省政府采购电子卖场采购方式：电子反拍 |
| 二〇二五年柒月 |

**目** **录**

第一部分 供应商须知 3

第二部分 采购需求 5

第三部分 附件 10

**第一部分 供应商须知**

1. **项目基本信息**

本项目分两个包，具体如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **分包** | **采购内容** | **最高限价（人民币元）** |
| 1 | A包 | 纳雍县人民医院网络安全设备维保服务：是对我院部分已有网络安全设备采购一年维保服务。 | 149,867.00 |
| 2 | B包 | 纳雍县人民医院网络安全设备：采购新增网络安全设备采购（含配套三年维保服务） | 259,019.00 |

**注：本项目两个分包意向供应商均须响应，不可单独响应报价或转包第三方。**

**一、供应商资格要求**

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.本项目的特定资格要求：无。

**二、竞价须上传资料**

参与本项目的供应商须于贵州省政府采购电子卖场平台竞价同时上传以下扫描件：

1.三证合一的营业执照副本（复印件加盖公章）；

2.法定代表人身份证明书附身份证复印件（格式详见“第三部分 附件”，法定代表人签字并加盖公章）；

3.如授权他人，授权委托书附身份证复印件（格式详见“第三部分 附件”，法定代表人签字并加盖公章）；

4.供应商资格承诺函（格式详见“第三部分 附件”，法定代表人或授权代表人签字并加盖公章）；

5.信用中国关于供应商的完整信用报告，生成日期须于竞价时间内，平台网址：https://www.creditchina.gov.cn/（信用报告须完整并加盖公章）。

6.报价函及报价一览表（报价一览表分A包、B包，缺一不可，格式详见“第三部分 附件”，法定代表人签字并加盖公章）；

7.网络安全设备原厂对供应商的投标资格授权函（加盖原厂公章）；

8.网络安全设备原厂家提供一年硬件质保与软件升级服务的售后服务承诺函（仅针对A包，格式自拟，加盖原厂公章）。

9.网络安全设备原厂家提供三年硬件质保与软件升级服务的售后服务承诺函（仅针对B包，格式自拟，加盖原厂公章）；

10.采购需求B包技术参数中要求提供的提供产品功能截图（加盖原厂公章）；

11.采购需求B包技术参数中要求提供的第三方检测报告（加盖原厂公章）。

**三、供应商审查**

竞价结束后，我单位将对报价的供应商进行审查，无效报价的情形如下：1.供应商未按竞价文件要求上传资料或上传资料不完整；2.供应商提供虚假资料应标；3.供应商被列入失信被执行人名单、税收违法黑名单、政府采购严重违法失信行为记录名单中；4.供应商上传报价函及报价一览表的报价与贵州省政府采购电子卖场平台的报价不一致；5.供应商报价超过项目预算。

注：如成交后发现供应商存在违法失信问题，我院将立即终止合同并追究相关责任。

**第二部分 采购需求**

1. 采购清单、技术参数

|  |
| --- |
| **A包（纳雍县人民医院网络安全设备维保服务）** |
| **序号** | **产品型号** | **ID** | **内容描述** | **数量** | **单位** |
| 1 | 终端安全管理系统(EDR) | / | 新增20套国产化PC端授权和30套国产化服务器端授权。 | 50 | 套 |
| 2 | 终端安全管理系统(EDR) | 1152302360 | 软件升级(服务器端) | 1 | 年 |
| 软件升级(PC端) | 1 | 年 |
| 3 | 终端安全管理系统(EDR) | 26117447324 | 软件升级(服务器端) | 1 | 年 |
| 软件升级(PC端) | 1 | 年 |
| 4 | GAP-1000-A600(网闻) | 5011045909 | 产品质保 | 1 | 年 |
| 软件升级(GAP-1000-A600 ) | 1 | 年 |
| 5 | DAS-1000-A620(数据库审计系统) | 0E84259B-5066003634 | 产品质保 | 1 | 年 |
| 软件升级 | 1 | 年 |
| 6 | AC-1000-C600-PT(全网行为管理) | CB2890D3-5038009486 | URL&应用识别规则库升级 | 1 | 套 |
| 软件升级 | 1 | 年 |
| 产品质保(标准版) | 1 | 年 |
| 7 | SIP-1000-E600(态势感知) | 4158227D-9W4P000291 | 深品质保全感知系统平台特征库软件 V2.0 | 1 | 套 |
| 软件升级 | 1 | 年 |
| 产品质保(标准版) | 1 | 年 |
| 8 | AC-1000-E440(上网行为管理) | F6CC096F-5077008378 | URL&应用识别规则库升级 | 1 | 套 |
| 软件升级 | 1 | 年 |
| 产品质保(标准版) | 1 | 年 |
| 9 | STA-100-A400(探针) | 7B788A10-5011045296 | 深信服安全感知系统探针特征库软件V2.0 | 1 | 套 |
| 软件升级 | 1 | 年 |
| 产品质保(标准版) | 1 | 年 |

|  |
| --- |
| **B包（纳雍县人民医院网络安全设备）** |
| **序号** | **设备名称** | **技术参数** | **数量** |
| 1 | SIP-Logger-A600(深信服日志分析管理系统) | 1、2U机架式硬件设备，配置≥6千兆电口，≥2万兆光口，配置单电源，配置可用存储量≥2TB；配置50个主机审计许可授权，最大可扩展审计主机数≥150个；2、设备平均每秒处理日志数（eps）≥2500。3、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于720种日志对象的日志数据采集；支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集；★4、支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射**（提供产品功能截图并加盖原厂公章）**；★5、支持网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到350条以上，支持自定义关联分析规则**（提供产品功能截图并加盖原厂公章）**；★6、支持日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量（**提供产品功能截图并加盖原厂公章）**；7、支持资产全生命周期管理，资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等，支持自定义资产标签、属性；8、内置主机安全报表（linux）、主机安全报表（windows）、 数据库安全报表、网络设备安全报表、应用安全报表五种；支持提供日报、周报、月报和自定义时间导出报表**9、提供至少三年硬件质保与软件升级服务，需提供原厂售后服务承诺函并加盖原厂公章。** | 1台 |
| 2 | YJ-1000-B1075(深信服云镜网络资产脆弱性扫描系统) | 1、1U机架式硬件设备，配置≥6千兆电口，≥2个千兆光口；配置单电源，配置硬盘容量≥128GB SSD+2TB SATA；2、设备支持资产发现最大并发IP数1024个，主机漏扫最大并发IP数150个，WEB漏扫最大并发URL数5个，基线核查最大并发IP数5个，弱口令扫描最大并发IP数150个；本次配置系统漏扫授权IP数100个，WEB漏扫授权URL数20个；3、支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持IOT资产扫描，EXCEL格式批量导入。★4、支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情**（提供产品功能截图并加盖原厂公章）**；★5、支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行**（提供产品功能截图并加盖原厂公章）**；6、支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入；7、支持检测的漏洞数大于300000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准。8、产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表**（提供产品功能截图并加盖原厂公章）**；9、支持国产数据库的漏洞扫描，包括神通、达梦、人大金仓、南大通用等。**10、提供至少三年硬件质保与软件升级服务，需提供原厂售后服务承诺函并加盖原厂公章。** | 1台 |
| 3 | OSM-1000-B1150(深信服运维安全管理系统) | 1、1U机架式硬件设备，配置≥6个千兆电口，单交流电源；要求配置50个资产运维授权数，最大可扩展资产运维授权数≥150个；2、设备图形运维最大并发数≥100，字符运维最大并发数≥200；3、支持多种协议的运维管理，如SSHv1、SSHv2、TELNET，RDP、VNC，FTP、SFTP、RDP磁盘映射、RDP剪切板等；4、支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用等；★5、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登录和审计接入**（提供产品功能截图并加盖原厂公章）**★6、支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别**（提供产品功能截图并加盖原厂公章）**7、支持调用本地数据库运维工具客户端，数据库类型包含mysql、oracle、sqlserver、SYBASE、INFORMIX、DB2、达梦V7、达梦V8、pgsql、kingbaseV7、kingbaseV8**（提供产品功能截图并加盖原厂公章）**8、支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开；9、具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚**10、提供至少三年硬件质保与软件升级服务，需提供原厂售后服务承诺函并加盖原厂公章。** | 1台 |
| 4 | 零信任综合网关aTrust-1000-B1030M | 1、1U机架式硬件设备，配置≥6个千兆电口，≥2万兆光口，单电源，配置硬盘≥128G SSD；2、最大理论加密流量（Mbps）≥300，最大理论并发用户数≥400，https并发连接数≥15000，理论https新建连接数（个/秒）≥60；加密最大流量（Mbps）≥85，配置接入授权≥350.3、为满足身份安全要求，应支持多因素认证，至少包括：账号密码认证、短信认证、证书认证、动态令牌认证、扫码认证，以及对接统一认证平台实现单点登录等认证方式。账号密码认证应支持设备自带账号密码认证，或通过LDAP/Radius/HTTPS协议对接第三方认证服务器。扫码认证应至少支持零信任客户端、企微、钉钉、飞书扫码认证。单点登录应支持标准的CAS、OAuth2.0、OIDC协议对接。为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：账号首次登录、账号在该终端首次登录、闲置账号登录、弱密码登录、异常时间登录、非常用地点登录等。4、为了保障用户在国产化终端上的正常业务访问，零信任客户端应兼容主流国产硬件CPU的国产操作系统终端，需提供国产操作系统与零信任厂商的兼容性证明，包括但不限于麒麟V10×龙芯、麒麟V10×龙芯LoongArch、麒麟V10×飞腾、麒麟V10×鲲鹏、麒麟V10×兆芯、麒麟V10×海光、麒麟V10×海思麒麟；统信V20×龙芯（3A3000、3A4000）、统信V20×龙芯（3A5000）、统信V20×飞腾、统信V20×鲲鹏、统信V20×海光、统信V20×兆芯、中科方德×飞腾、中科方德×海光、中科方德×兆芯、中科方德×龙芯3A5000等。5、为提升在弱网环境下访问体验，应支持优化TCP协议，增强隧道抗丢包、抗抖动特性，实现弱网环境的访问加速。**（提供产品功能截图并加盖原厂公章）**6、为降低业务访问时延，提升访问体验，应支持将短隧道资源新建连接耗时优化至 0RTT，大幅降低业务访问的网络时延，实现同等网络环境下访问速度接近甚至达到直连访问。**（提供产品功能截图并加盖原厂公章）**7、支持以虚拟IP方式，访问真实的业务系统，以便于审计设备区分访问用户。**（需提供第三方检测报告并加盖原厂公章）**8、支持以私有DNS发布企业资源，无需额外购买DNS服务即可使用域名访问内网资源，支持管理员自主配置是否允许从具体网络区域（局域网/互联网）接入时使用此私有DNS解析地址。9、应支持将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：账号安全、中间人攻击、SPA安全、cookie劫持等。**10、提供至少三年硬件质保与软件升级服务，需提供原厂售后服务承诺函并加盖原厂公章。** | 1台 |

二、商务要求

（一）售后服务：

1.针对本项目A包，网络安全设备原厂家提供一年硬件质保与软件升级服务的售后服务；

2.针对本项目B包，网络安全设备原厂家提供三年硬件质保与软件升级服务的售后服务；

3.按约定每季度进行现场巡检，检查设备硬件状态（如电源、风扇、接口）、软件配置（如策略有效性、版本兼容性）、日志完整性等。巡检后输出书面报告，针对问题提出整改方案并协助实施;

4.及时提供设备的官方固件、系统版本升级服务，确保漏洞修复、功能增强与厂商同步（需提前与用户确认升级计划，避免影响业务）。针对高危安全漏洞，需在漏洞公开后约定时间内（如 24 小时内）提供补丁安装服务，并验证修复效果;

5.当设备关联的系统发生安全事件（如入侵、攻击、数据泄露）时，供应商需协助用户进行事件分析（基于设备日志、告警信息），提供处置建议，并配合应急处置（如策略调整、流量拦截）。必要时提供专家级现场支持，参与事件溯源与止损;

6.提供 7×24 小时技术支持热线/在线渠道，解答用户关于设备配置、策略优化、功能使用等问题。如线上咨询及远程调试不能解决，需派遣经过技术认证的工程师赶赴现场解决技术问题，进行现场技术支持。

（二）供应商提供的货物及服务必须符合国家现行的相关规范、标准。

（三）供应商未按国家、行业规定及采购人要求完成服务，采购人可随时终止合同。

（四）合同签订后，由成交供应商与我院信息科联系相关事宜。

（五）项目报价不得高于我方最高限价，成交后报价即为合同价，报价含本项目所需一切费用。

（六）其余未定事宜合同约定。

**第三部分 附件**

附件一 报价函

附件二 报价一览表

附件三：供应商资格承诺函

附件四：法定代表人身份证明书、授权委托书（参考）

**附件一**

**报价函**

纳雍县人民医院：

我方参加贵单位组织的纳雍县人民医院网络安全设备及维保服务采购项目竞价采购，并进行报价。

一、按照《竞价文件》于贵州省政府采购电子卖场参与竞价并上传相关资料。

二、我方已完全理解《竞价文件》的全部内容。

三、本响应文件自竞价截止之日起90日内有效。

四、我方同意提供与报价有关的一切数据和资料。

五、联系方式：

联 系 人：

电 话：

地 址：

供应商全称：（盖章）

法定代表人（或授权代表）：（签字）

日期：2025年 月 日

第11页

**附件二**

**报价一览表（A包）**

项目名称：纳雍县人民医院网络安全设备及维保服务采购 金额单位：人民币元

第12页

| **序号** | **产品型号** | **ID** | **内容描述** | **数量** | **报价** | **备注** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 终端安全管理系统(EDR) | / | 新增20套国产化PC端授权和30套国产化服务器端授权。 | 1年 |  | 我方提供货物及配套服务均满足本项目竞价文件要求及采购人需求。 |
| 2 | 终端安全管理系统(EDR) | 1152302360 | 软件升级(服务器端) | 1年 |  |
| 软件升级(PC端) | 1年 |
| 3 | 终端安全管理系统(EDR) | 26117447324 | 软件升级(服务器端) | 1年 |  |
| 软件升级(PC端) | 1年 |
| 4 | GAP-1000-A600(网闻) | 5011045909 | 产品质保 | 1年 |  |
| 软件升级(GAP-1000-A600 ) | 1年 |
| 5 | DAS-1000-A620(数据库审计系统) | 0E84259B-5066003634 | 产品质保 | 1年 |  |
| 软件升级 | 1年 |
| 6 | AC-1000-C600-PT(全网行为管理) | CB2890D3-5038009486 | URL&应用识别规则库升级 | 1套 |  |
| 软件升级 | 1年 |
| 产品质保(标准版) | 1年 |
| 7 | SIP-1000-E600(态势感知) | 4158227D-9W4P000291 | 深品质保全感知系统平台特征库软件 V2.0 | 1套 |  |
| 软件升级 | 1年 |
| 产品质保(标准版) | 1年 |
| 8 | AC-1000-E440(上网行为管理) | F6CC096F-5077008378 | URL&应用识别规则库升级 | 1套 |  |
| 软件升级 | 1年 |
| 产品质保(标准版) | 1年 |
| 9 | STA-100-A400(探针) | 7B788A10-5011045296 | 深信服安全感知系统探针特征库软件V2.0 | 1套 |  |
| 软件升级 | 1年 |
| 产品质保(标准版) | 1年 |
| 合计 |  |

供应商全称：（盖章）

法定代表人（或授权代表）：（签字）

日期：2025年 月 日

**报价一览表（B包）**

项目名称：纳雍县人民医院网络安全设备及维保服务采购 金额单位：人民币元

第12页

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **报价** | **备注** |
| 1 | SIP-Logger-A600(深信服日志分析管理系统) | 1台 |  | **我方提供货物及配套服务均满足本项目竞价文件要求及采购人需求。** |
| 2 | YJ-1000-B1075(深信服云镜网络资产脆弱性扫描系统) | 1台 |  |
| 3 | OSM-1000-B1150(深信服运维安全管理系统) | 1台 |  |
| 4 | 零信任综合网关aTrust-1000-B1030M | 1台 |  |
| **合计** |  |

供应商全称：（盖章）

法定代表人（或授权代表）：（签字）

日期：2025年 月 日

附件**三**：供应商资格承诺函

供应商资格承诺函

致：纳雍县人民医院

我单位参加贵单位组织的项目名称纳雍县人民医院网络安全设备及维保服务采购的采购活动，根据竞价件要求,现郑重承诺如下:

1.符合《中华人民共和国政府采购法》第二十二条规定的条件：（1）具有独立承担民事责任的能力；（2）具有良好的商业信誉和健全的财务会计制度；（3）具有履行合同所必需的设备和专业技术能力；（4）有依法缴纳税收和社会保障资金的良好记录；（5）参加本次政府采购活动前三年内,在经营活动中没有重大违法记录；（6）符合国家法律、行政法规规定的其他条件。

2.我公司作为本项目参加采购活动的供应商、法定代表人/单位负责人近3年内不具有行贿犯罪记录。

3.我公司在截至投标截止日未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单。

4.我公司未违反“单位负责人为同一人或者存在直接控股、管理关系的不同供应商,不得同时参加本采购项目(包组)投标。为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商,不得再参与本项目投标。”的情形。

本公司对上述承诺的内容事项真实性负责。如经查实上述承诺的内容事项存在虚假,我公司愿意接受以提供虚假材料谋取中标追究法律责任。

供应商全称：（盖章）

法定代表人（或授权代表）：（签字）

日期：2025年 月 日

附件**四**：法定代表人身份证明书、授权委托书（参考）

法定代表人身份证明书

单位名称：

单位性质：

地 址：

成立时间： 年 月 日

经营期限：

姓名： 性别： 年龄： 职务：

系 （供应商单位名称） 的法定代表人。

特此证明。

**法定代表人身份证反面**

**（人像）**

### 法定代表人身份证正面

**（国徽）**

供应商全称(单位公章):

供应商法定代表人（签名或签章）：

日 期: 2025 年 月 日

授权委托书

致：纳雍县人民医院

兹委派我单位（被委托人姓名）参加贵方组织的纳雍县人民医院网络安全设备及维保服务采购的采购活动，全权代表我单位处理本次采购中的有关事务，该人员在采购中的所有行为，我单位均予承认。

本授权书于盖章签字之日起生效。

特此委托

附全权代表情况：

姓名：性别：身份证号码：

部门：职务：

通讯地址：邮政编码：

电话：传真：

其他联系方式：

法定代表人：（签名或签章）

供应商全称：(单位公章)

2025年 月 日

（注：后附法人身份证及被委托人身份证复印件）