**云南省中医中药研究院**

**院内项目竞争性磋商文件**

项目名称： 云南省中医中药研究院信息系统二级等保云安全产品及服务

项目科室： 院办公室

发放日期： 2023 年 11 月20日

**第一章 竞争性磋商邀请**

根据《云南省中医中药研究院采购管理办法（试行）》，对 云南省中医中药研究院信息系统二级等保云安全产品及服务（项目名称）采用竞争性磋商方式发包，项目资金来源 财政经费 ，资金落实情况 已落实 。现邀请合格的供应商参加报价和磋商。

项目编号： szyycg2023024

项目名称： 云南省中医中药研究院信息系统二级等保云安全产品及服务

项目预算金额： 44000元

响应性文件份数： 1 份

递交响应性文件截止时间：2023年11月28日10时00分

递交地点： 五台路2号2号楼408室

响应性文件接收人： 陈果

磋商时间：2023年11月28日10时00分

磋商地点： 五台路2号三楼会议室

届时请参加谈判的单位法定代表人或法人委托人参与磋商。

联系人：陈果

联系电话：0871-65190525

**第二章 竞争性磋商须知**

一、采购需求（主要包括采购项目的技术规格、数量、服务标准、验收等要求）

## 1、项目概括

云南省中医中药研究院现有独立委托开发的信息系统3个，采购的云安全产品及服务需满足达到集成3个不同信息系统的网络安全等级保护测评2.0的相关要求，并具有扩充融合更多系统（不超过6个系统）的能力空间，并提供持续网络安全防护服务。本项目采购预算为：44000元/年。服务期限为签订合同起3年。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品** | **数量** | **单位** |
| 1 | 防火墙即服务 | 1 | 套 |
| 2 | 入侵防护即服务 | 1 | 套 |
| 3 | 日志审计即服务 | 1 | 套 |
| 4 | Web应用防护服务 | 1 | 套 |
| 5 | 主机漏洞评估服务 | 2 | 次 |
| 6 | 堡垒机服务 | 1 | 套 |
| 7 | 态势中心 | 1 | 套 |

2、需执行的国家相关标准、行业标准及规范：

供应商提供的货物或服务符合国家相关质量标准、规范及采购文件要求。

3、服务质量要求（或考核标准）：

满足网络安全等级保护测评2.0测评的相关要求，开展安全运维管理。

5、项目验收要求：

 确保信息系统满足网络安全等级保护测评2.0测评的相关要求，通过备案。

二、供应商须知

|  |  |
| --- | --- |
| **项目名称** | 云南省中医中药研究院信息系统二级等保云安全产品及服务 |
| **资金来源** | 财政性资金 |
| **资金落实情况** | 已落实 |
| **服务期限** | 自合同签订起一年以内 |
| **付款方式** | 一次性付款 |
| **分包及成交规定** | ☑本项目不分包 |
| **供应商资格要求和资质条件、能力** | 资质条件：具备独立完成本项目的营业范围、资质及同类项目实施经验。 |
| **是否接受联合体投标** | ☑不接受 |
| **供应商不得存在的其他情形** | 1. 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，不得参加同一项下的政府采购活动；
2. 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。
 |
| **提交响应文件截止日期** | 2023年11月28日10时00分 |
| **响应文件份数** | 1套 |
| **响应文件组成** | （1）资格审查文件；（2）供应商法人代表身份证明、经办人身份证复印件、经办法定代表人授权委托书，加盖公章；（3）供应商必须按谈判要求提供报价表；（4）其他相关材料（根据采购项目实际需求）。 |
| **递交响应文件地点** | 五台路2号2号楼408室 |
| **磋商时间和地点** | 五台路2号2号楼三楼会议室 |
| **磋商规则** | （1）供应商按抽签顺序进行报价和答疑；（2）评审专家组成：由院内3人以上（单数）组成；（3）谈判实质性响应供应商原则上不少于三家,方可正式开始磋商；（4）经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。 |
| **评审方法** | 综合评分法 |
| **结果公告** | 公告媒介：云南省中医中药研究院官网公告期限：1个工作日 |
| **质疑期** | 供应商认为磋商文件、磋商过程和结果使自己的权益受到损害的，可以在知道或者应知其权限受到损害之日起7个工作日内，以书面形式向采购人提出质疑。 |
| **质疑答复** | 采购人在收到供应商的书面质疑后七个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复内容不得涉及商业秘密。 |

第三章 供应商应当提交的资格证明文件

资格证明文件目录

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 证明材料 | 备注 | 必须提交 |
| 1 | 营业执照、登记证书、执业许可证等 | 具有独立承担民事责任能力的企业或组织合法经营权的凭证（如营业执照、登记证书、执业许可证等）的原件扫描件 | √ |
| 2 | 供应商法人代表身份证明、经办人身份证复印件、经办法定代表人授权委托书，加盖公章 | 原件 | √ |

备注：

1、必须提交的证明材料未提交或提交不全的视为资格性审查不合格。

2、供应商的资格证明材料应当真实、有效、完整，字迹、印章要清晰

第四章 评分方法

**一、综合评分**

评审委员会按以下公式计算出各磋商申请人的总得分，推荐成交候选人按评审总得分由高到低顺序排列；评审总得分相同的，按磋商报价由低到高顺序排列；评审总得分且磋商报价相同的，按技术指标优劣顺序排列，依次类推。

评标总得分F1×A1＋F2×A2＋……＋Fn×An

F1、F2……Fn分别为各项评分因素的汇总得分；

A1、A2、……An 分别为各项评分因素所占的权重(A1＋A2＋……＋An＝1)。

其中F值为评标委员会所有成员汇总得分的算术平均值。

投标报价 F1：100 分，权重 A1为 0.1

技术部分F2：100 分，权重 A2 为 0.5；

商务部分F3：100 分，权重 A3 为 0.4

|  |  |  |
| --- | --- | --- |
| **序号** | **评审项目** | **评分标准** |
| 1 | F1投标报价得分(满分为100分) | 报价得分=(评标基准价／磋商报价)×100 |
| 2 | F2技术部分评分标准(满分为100分) | 技术参数（满分50分） | 第一个档次（50分）：技术参数响应性优，有正偏离，无负偏离项；第二个档次（40分）：技术参数响应性较好，无负偏离项；第三个档次（30分）：主要技术参数响应性一般，基本满足要求。 |
| 质量保证及承诺（满分30分） | 第一个档次（30分）：质量保证及承诺优，措施完善；第二个档次（20分）：质量保证及承诺良好；第三个档次（10分）：质量保证及承诺一般。 |
| 实施方案及进度安排（满分20分 | 第一个档次（20分）：实施方案及进度安排（包括交货、安装调试及验收等各项工作，下同）完善具体、合理可行，针对性强；第二个档次（15分）：实施方案及进度安排合理可行，有一定的针对性；第三个档次（10分）：实施方案及进度安排基本可行，针对性不足。 |
| 3 | F3商务部分评分标准（满分100分） | 类似业绩（50分） | 第一个档次（50分）：供应商近三年类似项目业绩优；第二个档次（40分）：供应商近三年类似项目业绩良；第三个档次（30分）：供应商近三年类似项目业绩一般。 |
| 售后服务方案、承诺及保证（满分30分） | 第一个档次（30分）：售后服务方案、承诺及保证完善具体，针对性强；第二个档次（20分）：售后服务方案、承诺及保证具体可行，有一定的针对性；第三个档次（10分）：售后服务方案、承诺及保证基本可行，但缺乏针对性。 |
| 社会信誉（满分20分） | 第一个档次（20分）：社会信誉优；第二个档次（15分）：社会信誉良好；第三个档次（5分）：社会信誉一般。 |

**二、评审总得分的计算**

（1）评审时，评审委员会各成员独立对每个有效磋商人的磋商文件进行评价、打分，然后汇总每个磋商人每项评分因素的得分。

（2）F评审总得分＝F1＋F2＋……＋Fn

　　F1、F2……Fn分别为各项评分因素的汇总得分；

其中F值为评审委员会所有成员汇总得分的算术平均值。

附件2

**云南省中医中药研究院采购项目供应商报价表**

采购项目名称： 云南省中医中药研究院信息系统二级等保云安全产品及服务 货币单位：人民币元

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **规格及技术标准、服务内容** | **数量** | **单价** | **总价** | **偏离情况说明** |
| 1 | 防火墙即服务 | 1、提供防火墙防护配置, 可按源地址、目的地址、应用、服务进行策略配置； 2、可配置防火墙策略中应用协议服务项目内容；3、可配置防火墙策略所操作的地址库，支持IP、IP范围、子网；4、内置应用识别库，支持网络应用类、媒体类、视频类等应用识别，并可在一体化策略中引用，实现一体化的防护效果；★5、支持应用过滤器，至少支持4个维度进行过滤，比如：应用类别、实现技术、风险等级、标签；★6、能够在一条策略里配置源/目的IP地址/MAC地址/IP池/域名、安全区、应用/应用组、协议/端口、时间、用户、安全模板/模板组；7、提供从网络层、应用层到内容层的深度安全检测能力，基于安全策略有效阻断恶意攻击。★8、支持1000+万级的病毒库，病毒查杀率高。 | 1套 |  |  |  |
| 2 | 入侵防护即服务 | 1. 在防火墙的配置策略下,可配置入侵防护功能；2、系统需提供至少10种以上内置规则模板，帮助用户快速上线。如DMZ区服务器、内网客户端、Web服务器、Windows服务器、UNIX服务器防护等规则模板，并可根据内置规则模板直接派生模板；★3、系统攻击特征库数量为1万+；★4、支持多种威胁情报场景，包括APT检测/挖矿检测/勒索检测/反诈检测/失陷检测/暗网节点检测；5、系统应能够有效抵御SQL注入、XSS注入、webshell等多种常见的应用层安全威胁，并可配置SQL注入白名单。
 | 1套 |  |  |  |
| 3 | 日志审计即服务 | 1、可对环境中的全量日志进行收集与存储，可满足等保2 0、网络安全法中有关日志留存的要求；对于存储的日志信息进行了完善的保护，避免遭受不法分子的删除及修改；2、可对日志概览进行展示, 包括所有资产的日志总数、事件总数、告警总数、拦截总数、日志接入信息、日志类型等，并可按资产和时间周期对日志进行过滤展示；3、提供日志源配置，支持windows/linux主机日志采集，可按资产对日志进行接入,并可管理已接入的设备；★4、系统应支持日志源监控能力，包括采集器维度及资产维度的监控，资产维度支持展示资产详细信息。★5、系统应内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别。 | 1套 |  |  |  |
| 4 | Web应用防护服务 | ★1、支持HTTP 1.0/1.1，且可根据现网环境配置协议降级；2、支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell及Ruby shell，同时可支持源IP封禁、Session封禁和UA封禁；3、支持XML防护，包括XML基础校验、Schema校验以及SOAP校验。4、支持人机识别，可通过JS脚本识别自动化工具，并能够对自动化工具访问请求配置放过、阻断、接受、伪装等处置动作。可以根据客户端环境检测，识别攻击工具，主要包括：市面上主流扫描器，如burpsuite、nessus等，市面上主流自动化工具selenium、phantomjs等，脚本攻击识别；★5、支持对攻击源地址的智能阻断，支持永久封禁或者自定义IP封禁时间（秒/分钟/小时），并且可以手工解除解禁。 | 1套 |  |  |  |
| 5 | 主机漏洞评估服务 | 1、可针对主机资产进行扫描任务下发操作，扫描执行完成后, 可在防护配置页下载扫描结果；2、支持扫描操作系统、数据库、中间件等多种资产；3、提供多维度、多方式的分析报告，帮助用户快速定位风险类型、区域、严重程度，海量数据中高效定位具体资产漏洞；4、可查询该服务对应的订单号、订单类型、时间；★5、支持检测的漏洞数大于250000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准。★6、内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术。 | 2次 |  |  |  |
| 6 | 堡垒机服务 | 1、系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约，缺省用户账号密码遗失后仅能被重置；2、支持托管设备按管理员进行分权管理，支持同一个设备可分配给不同的管理员进行管理，防范出现权限管理瓶颈，即单个设备管理员不在后无人管控相应设备权限；3、半自动登录目标设备：即第一次登录目标设备时运维人员需手工输入目标设备帐号和密码并允许堡垒机保存该帐号密码，运维人员就可以自动登录目标设备；★4、支持自动发现运维人员运维过程中创建的后门账号行为，并以列表方式向设备管理员展示托管设备中所有的后门账号信息；5、支持实时监控通过SSH、SFTP、RDP、VNC 、Telnet、FTP、X11等协议的操作行为；对监控到的非法操作，可实时手工切断。 | 1套 |  |  |  |
| 7 | 态势中心 | 1、态势中心具有态势感知大屏，对当前网络环境整体安全态势进行展示，以便用户了解当前网络环境。包括运营态势大屏、存在漏洞的资产、阻断外部攻击次数、攻击者 IP 数量、已处置安全事件数量、攻击阻断趋势、事件闭环率、事件闭环趋势；2、资源管理：包含设备查询、添加设备、设备升级、资源告警、配置备份、配置恢复等功能；3、引流管理：可新建域名/IP 引流申请，经审核通过后，可将客户的业务流量牵引到资源池，通过资源池的安全能力，对流量进行安全防护。 | 1套 |  |  |  |

注：标注★为关键项目，需提供功能界面截图证明并加盖厂商公章。

报价供应商名称（公章）： 地址：

报价供应商项目技术负责人（签字）： 联系电话：

电子邮箱： 报价日期： 年 月 日