**湛江市霞山区人民法院**

**网络安全等级保护二期设备采购**

**项目竞价文件**

竞价项目：湛江市霞山区人民法院网络安全等级保护二期

设备采购项目

编制单位：湛江市霞山区人民法院

编制时间：2022年6月24日

项目竞价说明及要求

发布机构:湛江市霞山区人民法院采购小组

采购方式:竞争性谈判采购  采购编号:XF20220624

采购品目: 湛江市霞山区人民法院网络安全等级保护二期设备采购项目

网络安全等级保护二期设备采购项目项目采用竞争性谈判采购，欢迎符合资格条件的供应商参加。

一、采购项目编号：XF20220624

二、采购项目名称：湛江市霞山区人民法院网络安全等级保护二期设备采购项目

三、采购预算：320000元

四、项目内容及需求：(采购项目技术规格、参数及要求)

1、项目内容：网络安全等级保护设备采购

2、用途：网络安全等级保护

3、数量：2台

  4、竞价文件见附件

http://www.xsfy.gov.cn/include/ueditora/dialogs/attachment/fileTypeImages/icon_doc.gif[湛江市霞山区人民法院网络安全等级保护二期设备采购项目](http://www.xsfy.gov.cn/uploads/20210824/1629769601838260.docx" \o "湛江市霞山区人民法院综合布线系统升级改造项目竞价文件.docx)

**五、供应商资格：**

1.报价人应具备《政府采购法》第二十二条规定的条件。

2.报价人在中华人民共和国境内注册的能独立承担民事责任的法人或其他组织，取得合法企业工商营业执照、税务登记证、组织机构代码证（或三证合一）。

**六、投标时间：**符合资格的报价人请于2022年6月29日下午3:00点前，委派法定代表人到湛江市霞山区人民法院808室提交参加竞标文件资料。

**七、报名方式**为现场报名，报名时需提交以下材料，无误后办理报名登记：

1. 报价表（复印件加盖公章，原件备查）、联系人及联系人电话。

**八、投标截止时间及开标时间：**2021年6月29日下午3:30（北京时间）。

**九、谈判地点：**湛江市霞山区人民法院808室

**十一、评标方式：**按实际到场家数或符合招标条件家数进行现场谈判。

**十二、公告地点：**广东省湛江市霞山区人民法院门户网站公告栏

采购人名称：广东省湛江市霞山区人民法院

电话：0759-2368978   传真：0759-2368979

湛江市霞山区人民法院

2022年6月24日

附件一 报价表格式

**竞价报价书**

**湛江市霞山区人民法院：**

1、根据你方湛江市霞山区人民法院网络安全等级保护二期设备采购项目的竞价文件，经考察项目现场研究上述项目竞价文件所有条款后，现投送该项目竞价书，我报价： 元，按竞价文件之规定范围与条件以及竞价文件所有条款的承诺，承担责任。

2、一旦我公司入围，我方保证在接到中标通知后在要求时间内采购，在限定日期　 　　日历天内完成并移交合同规定的全部货物。

竞价人：（盖章）

法定代表人：（签字或印鉴）

日期： 年 月 日

附件二 **项目需求清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **技术参数要求** | **数量** | **单位** | **单价（元）** |
| 1 | 数据库审计 | 最大硬件吞吐量≧2Gbps，最大数据库纯SQL流量≧400Mb/s，数据库实例个数不少于30个，SQL处理性能≧30000条SQL/s，日志检索性能≧500000条/秒。规格：1U，内存大小≧8G，硬盘容量≧2T SATA，电源：单电源，接口≧6千兆电口+2万兆光口SFP+。  含：数据库安全审计系统软件 (\*1套);产品质保(\*3年);软件升级(\*3年);  技术要求：  1、要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁；  2、B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端；  3、支持主流数据库Oracle（Tdata）、SQL-Server、DB2、MySQL（Tdsql）、Informix、Sybase、Postgresql、Cache、MongDB、K-DB，虚谷；  4、支持通过SQL串模式抽取保障磁盘IO的读写性能；分离式存储SQL语句保障数据审计速度快；  5、内置大量SQL安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表等； | 1 | 台 | 157000 |
| 2 | 安全感知管理平台一体机(SIP一体机) | 网络层吞吐量：≤500Mbps；规格：1U，内存大小≧16G，硬盘容量≧128G MSATA+4T SATA，电源：单电源，接口≧6千兆电口+2万兆光口SFP+。 含：安全感知管理平台软件（\*1套）;安全感知系统平台特征库软件（\*2套）;产品质保(\*3年);软件升级(\*3年);  技术要求：  1、基于审计的流量元数据，利用机器学习、人工智能、威胁情报、沙盒检测、特征分析等方法进行威胁检测的整个过程。同时，能以安全事件视角和服务器/终端视角直观的看清内网安全状况；  2、具备失陷(业务和服务器)主机详细分析，包含攻击阶段分布、风险等级趋势、安全事件举证、开放端口等信息。攻击阶段包含存在漏洞、遭受攻击、C&C通信、黑产牟利、内网扫描、内网扩散、盗取数据支持对每个安全事件详细举证分析，包含风险危害、处置建议、专杀工具等；  3、支持对威胁情报的安全告警做专项性分析，比如通过情报匹配的风险主机分布、威胁趋势分析，将发生的所有安全事件默认按照处置状态，威胁等级，确定性等级，攻击结果、事件类型等维度进行筛选展示，并结合攻击阶段、事件统计和事件趋势等进行统计和显示、可实时监控发生的安全事件；  4、支持文件威胁分析，可展示文件分析过程、文件检测趋势、恶意文件TOP5；支持恶意文件的详情分析，包括支持记录恶意文件感染的主机、所属IP、文件名、病毒名称、传输协议等；支持导出文件威胁分析结果；  5、支持完整展示网络的安全态势和详情的综合风险报告，报告内容包括系统说明、安全风险概括、业务与终端安全详情分析、安全规划建设建议等。 | 1 | 台 | 163000 |
| **总计** | | | | | 320000 |