**阳江市人民检察院工作网移动存储交换服务平台建设项目**

**招标文件**

阳江市人民检察院

二〇二〇 年十一月

# 第一部分 报价邀请

根据阳江市人民检察院工作网移动存储交换服务平台建设需要，我院就该项目进行邀请招标采购，现通过我院外网发布公告，邀请符合资格条件的供应商参加。有关事项如下：

1. 采购项目概况：
2. 项目名称：阳江市检察机关工作网移动存储交换服务平台建设项目
3. 采购预算：341363.51元
4. 采购方式：邀请招标
5. 项目内容及需求：阳江市人民检察院工作网移动存储交换服务平台建设（具体内容及要求详见用户需求书）
6. 完工期：合同签订生效后60个日历天内完成。
7. 项目地点：阳江市人民检察院。
8. 供应商资格：

**注：投标人投标时须提供营业执照原件核查，否则将作无效投标处理。**

1. 投标人应具备《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）法律、行政法规规定的其他条件。

1. 投标人须是中华人民共和国境内合法注册，能独立承担民事责任并具有相关经营范围的法人；
2. 本项目不接受联合体投标，不允许投标人对本招标项目进行分包和转包；
3. 招标时需提交的资料（用信封密封盖章）

（1）、中华人民共和国法人证书副本复印件或企业法人营业执照副本复印件

（2）投标人在广东省政府采购网备案及定点采购台式计算机供应商资格的网页截图

（3）报价方案，投标人根据设备的实际报价及选用技术参数优于或等于的产品进行投标，并列明详细的技术参数、品牌、型号及产地等。

1. 评标办法，经评审报价最低者中标

五、招标响应文件递交截止时间及地点：

1. 招标响应文件递交时间：2020年 11 月 18 日上午9：30（北京时间）。提前、逾期递交或递交不符合规定的邀标文件恕不接受。
2. 招标响应文件递交截止时间、评标时间：2020年 11 月 18 日上午9:30 (北京时间)。
3. 招标响应文件递交地点：阳江市人民检察院1号楼四楼会议室
4. 采购人、采购代理机构的名称、地址和联系方式

名 称：广东省阳江市人民检察院

联系人：郑经华

联系电话：0662-3360076

第二部分 用户需求书

**A.商务要求**

**一、报价要求：**投标报价应为人民币含税全包价，包括安装、测试、调试、培训、质保期（维护期）服务、各项税费及合同实施过程中不可预见费用等。**投标总报价不得高于341363.51万元人民币。（超出该上限的投标报价将作为无效投标处理）**

**二、项目基本要求：**成交供应商应保证产品或产品任何部分非他人所有或与他人共有，未设有抵押权、租赁权，未侵犯他人的专利权、版权、商标权等知识产权。一旦出现侵权，成交供应商应承担全部责任。成交供应商必须保证产品符合相关验收标准，并通过验收后，再移交采购人。

**三、完工期：**合同签订生效后60个日历天内完成。

**四、服务地点：**采购人指定地点。

**五、维护期：**质保期为自项目终验收完成之日起三年。成交供应商负责维护期内的免费升级服务，质保期、运维期内，出现故障，成交供应商须派出技术工程师到达现场处理故障，并承担一切费用。

**六、付款方式：**

合同签订后，采购人向供应商支付合同金额30%，供应商开始进场实施，30个日历天内完成设备（软硬件）进场，采购人清点设备无误后向供应商支付合同金额40%。签合签订后60个日历天内，供应商完成实施并交付验收（供应商提供验收报告由采购人盖章），验收合格后采购人向成交供应商支付合同金额25%。验收合格后一年内，采购人向供应商合同金额的5%。成交供应商凭以下有效文件与采购人结算：

1、合同；

2、成交供应商开具的正式发票；

3、中标公告。

**七、项目实施、验收**

1、项目实施管理

供应商须具有成熟实施能力，并且提出有效的实施方案。项目主要开发人员需具有承担过相关系统软件开发经验，能够与用户进行良好的沟通，要熟悉系统开发架构。

供应商应在项目实施过程中，承诺做到：

（一）根据项目进展及时向采购人报审进度文档。

（二）系统开发基于服务提供的应用支撑平台。

（三）系统设计必须满足的相应标准规范。

2、试运行及验收

成交供应商应按软件项目整体验收要求和验收流程完成验收准备，应协助完成整体验收。

（1）试运行：项目中各子系统并行开发，每个子系统完成研发及测试工作后，交采购人试运行，分批完成系统试运行。

（2）合同验收：成交供应商在60个日历天内完成系统的交付，再由成交供应商提出验收申请，由采购人根据本系统总体设计的要求，从系统功能、性能，文档等几方面进行验收。

（3）验收标准：以《合同》《采购文件》《报价方案》《系统需求规格说明书》为依据，供应商根据项目验收标准完成相应工作并保障所开发系统无故障运行并经采购人确认，由采购人按照技术方案和有关规定组织验收。

（4）移交与本项目有关的相关技术资料，包括文档资料和程序等。

**八、售后服务**

1、售后服务依据

以《合同》《采购文件》《报价方案》《系统需求规格说明书》为依据，在系统验收交付后，三年内成交供应商对项目需求范围内提供免费修复、整改与开发支持。

2、售后服务内容：项目需求范围内的系统问题、异常与缺陷的开发支持。

3、供应商要提供远程技术服务和现场技术服务。远程技术服务以电话、传真、Email等方式提供7\*24小时响应。如采购人需要提供现场技术服务，在4小时内安排技术工程师到达用户方现场提供现场技术服务。对于不能及时修复的运行服务，系统商负责提供妥当的服务转移，以使整个软件系统能够提供不间断的服务并在24个小时内予以解决。

**B.技术要求**

**1、★投标文件的响应内容均真实有效，且按原厂商设备参数进行响应，不存在虚假响应内容或设备技术指标前后参数响应矛盾的情况，否则将被视为无法实质性响应招标文件而作废标处理。对招标需求中的所有条款，投标人如在投标时承诺满足，但中标后发现有虚假响应，即事实上不能满足的，采购人将取消投标人的中标资格。**

2、招标需求中标注有“★”号的条款必须实质性响应，负偏离（不满足要求）将导致投标无效。

3、招标需求中标注有“▲”的条款为重要条款，要求投标人提交相关证明材料，如没有证明材料或专家认定证明材料无效的，该条款视为不满足，采购人有权取消投标人的中标资格。

**★**4、对招标需求中的所有条款，投标人如在投标时承诺满足，但中标后发现有虚假响应，采购人有权邀请第三方机构对招标需求中的所有条款进行逐一验证，所产生费用由投标人承担，即事实上不能满足的，采购人有权取消投标人的中标资格。

## 采购产品清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **组件** | **品牌型号** | **描述** | **数量** | **单位** |
| 1 | 数据安全交换中间机系统 | 硬件（台式机） | 可选：长城世恒KF510，联想开天S720Z，超越申泰DT3000-F，浪潮英政CE2110G1。 | 自主可控国产化方案 ，配置飞腾FT-1500A 1.5GHz 4核处理器、8G内存, 240GB硬盘，1G独立显卡，21寸以上显示器，提供3年整机质保，符合国产保密要求。  详细参数要求见“2.3.1中间机硬件配置要求”章节描述。 | 13 | 台 |
| 2 | 操作  系统 | 银河麒麟 | 银河麒麟V4.0.2系统正版授权。 | 13 | 套 |
| 3 | 防病毒  模块 | 安天智甲 | 专用机防病毒系统 | 13 | 套 |
| 4 | 主机监控与审计系统模块 | 交大捷普 | 硬件监控、移动存储设备监控、文件监控、网络监控、身份认证。  详细参数要求见“2.3.2主机监控与审计模块功能要求”章节描述。 | 13 | 套 |
| 5 | 数据交换系统模块 | 交大捷普 | 移动存储介质配套系统软件，部署于中间机上，自动导入导出、可控安全交换、强制病毒查杀、强制访问控制、单机版主审日志推动等功能。  详细参数要求见“2.3.3中间机数据交换系统模块功能要求”章节描述。 | 13 | 套 |
| 6 | U盘注册管理系统 | 交大捷普 | 移动存储介质注册、管理、环境配置、日志服务配置等等  详细参数要求见“2.3.4 中间机U盘注册管理系统功能参数要求”章节描述。 | 1 | 套 |
| 7 | 原终端安全管理系统升级技术服务 | 跨版本  升级 | 交大捷普 | 1、将原有的主机监控与审计系统（基础版）升级为主机监控与审计系统（移动外设版）。  2、服务期内提供更换新产品软件授权点700个（一年）。  详细参数要求见“2.3.5原终端安全管理系统升级版本功能要求”章节描述 | 1 | 套 |
| 8 | 客户端升级 | 交大捷普 | 因产品跨版本升级，需现场升级服务，重新安装市院服务器端系统和150个客户端软件。  提供产品升级服务、原厂安装服务。 | 1 | 项 |
| 9 | 移动存储交换介质 | 安全可控U盘（外网版） | 交大捷普 | 专用安全U盘32G。防复制、防篡改、防病毒、防截屏录屏、防暴力破解、限时限次、文件隐藏等功能  详细参数要求见“2.3.6安全可控U盘技术参数要求”章节描述 | 120 | 个 |
| 10 | 安全可控U盘（内网版） | 交大捷普 | 专用安全U盘32G。登陆认证、强制标记认证、安全审计、日志上次数据中心、支持Linux、Windows跨平台使用。  详细参数要求见“2.3.6安全可控U盘技术参数要求”章节描述 | 120 | 个 |

### 中间机硬件配置要求

|  |  |
| --- | --- |
| CPU | 飞腾FT1500A 4核或以上处理器 |
| 操作系统 | 麒麟桌面操作系统 |
| 固件 | 国产昆仑固件 |
| 硬盘 | 240GB 以上硬盘 |
| 内存 | DDR4 8GB |
| 2个内存插槽 |
| 光驱 | 内置DVD刻录光驱 |
| 接口 | 前置2个USB2.0接口 |
| 后置4个USB3.0接口 |
| 独立显卡，1G显存，带VGA和HDMI接口 |
| 电源 | 交流供电电压220V |
| 显示器 | 21.5寸LED屏 |

### 中间机主机监控与审计模块功能要求

|  |  |  |
| --- | --- | --- |
| 管理用户分级 | 采用“三权分立”的用户管理权限：分别是系统管理员、安全保密管理员和安全审计员，可对各自不同的权限管理和日志管理等。 | |
| 多操作系统支持 | ▲可支持银河麒麟桌面操作系统、中标麒麟桌面操作系统（龙芯、兆芯），支持飞腾FT-1500A/4 1.5GHz(4核)、龙芯3B1500 1.2GHz (8核)、兆芯ZX-C4610 2.0GHz(4核)等CPU，（提供证明材盖原厂盖章证明） | |
| 基础环境审计 | 软件变更审计 | 监控终端软件安装及卸载行为 |
| 硬件变更审计 | 监控终端硬件变更行为，硬件设备类型包括CPU、主板、键鼠、硬盘等系统自身硬件 |
| 软件安装控制 | 对终端安装软件进行控制，禁止黑名单软件安装 |
| 登录审计 | 登录审计 | 监控终端的开机、关机、注销及登录行为 |
| 外设审计 | 移动存储介质控制 | 监控终端接入的移动存储介质，包括允许、只读和禁止 |
| 打印审计 | 监控终端的打印行为 |
| 刻录审计 | 监控终端的文件光盘刻录行为 |
| 外围接口控制 | 禁止终端使用USB设备，包括光驱、USB、打印机等 |
| 网络审计 | 端口审计 | 对终端端口进行黑白名单监控，阻断黑名单端口监听行为 |
| 网络连接审计 | 对终端网络连接行为进行黑/白名单式的管理。按网络五元组（协议、源IP、源端口、目的IP、目的端口）等信息，对网络行为进行审计，支持TCP、UDP、ICMP等网络协议。 |
| 网络限制 | 限制终端与未受控主机的连接 |
| 文件审计 | 文档审计 | 对终端的文件操作行为进行审计，操作类型包括：修改、复制从、复制到、重命名（同盘剪切）和删除；文件存储位置包括本地磁盘、移动硬盘、U盘、红盘和网络共享；文件类型包括：文件、扩展名及目录 |
| 系统安全审计 | 系统安全审计 | 审计国产版操作系统安全相关的事件，包括软件安装卸载事件、安全策略变更事件、可执行程序加载事件、违反操作系统访问控制策略、身份鉴别、安全审计相关事件、其他系统安全事件 |
| 进程审计 | 进程流量审计 | 对终端进程的上传流量、下载流量进行监控，当上传流量或下载流量超出策略配置的阈值时，将产生审计日志 |
| 进程基础审计 | 对终端运行的系统进程进行监控 |
| 进程行为审计 | 对指定进程做进程信息采集，包括创建的子进程信息、对文件操作的信息、进程的网络行信息等 |
| 进程控制 | 对指定进程做应启动和应关闭控制 |
| 系统服务审计 | 服务监控审计 | 对终端上的系统服务进行监控，包括开启和关闭配置的服务，并将信息记入审计日志 |
| 时间同步 | 对终端时间进行同步，包括系统时间监控类型：按时间源进行同步（需填写时间源IP）、与服务器进行同步，时间同步监控类型：按间隔周期同步（需填写间隔周期）、按时间点同步（需填写具体时间） |
| 开关机监控 | 对终端非授权时间开关机进行监控，监控类型包含：记录、不监控，当选择记录时，可勾选记录授权开关机行为，可选取开关机授权时间段 |
| 账户监控 | 监控终端账户变更情况 |
| 异常行为审计 | ARP监控审计 | 识别ARP攻击，同时可检测IP地址冲突问题，可自定义防御机制，自动、手动绑定网关IP/MAC，对网关欺骗、一般欺骗、带宽限制的行为进行审计 |
| 端口扫描 | 对端口扫描的恶意行为进行检测，可配置是否防御功能 |
| 主机安全 | 对终端安全策略进行审计，包括密码长度、密码复杂度、密码口令周期、尝试失败次数、杀掉软件和关键目录安全策略配置 |
| 系统管理 | 客户端软件自我保护 | 防止客户端软件被卸载或失效。 |
| 自动备份管理 | 具有自动备份功能，可根据需要自动执行备份任务，实现实时数据自动备份，有效防止数据丢失 |
| Syslog审计 | 可将日志发送第三方Syslog |
| 终端管理 | ▲主机信息获取 | 能够获取终端的资产信息，包括系统信息、资源性能信息、进程信息、服务信息、系统事件信息、共享目录信息、网络连接信息、浏览器访问信息、帐户信息和最近下发的策略信息。其中在进程信息中能够关闭某个进程的运行，在共享目录中能够关闭某个共享的目录（提供界面截图证明加盖原厂商公章） |
| 日志报警、查询功能 | 支持日志信息报警、查询功能，管理员能够通过输入时间、所在模块、级别、日志类型等查询条件，对所有日志进行分类查找 | |
| ▲产品证书 | 1）公安部《计算机信息系统安全专用产品销售许可证》（三级）  2）产品具有国家保密局《涉密信息系统产品检测证书》 | |

### 中间机数据交换系统模块功能要求

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标技术参数** |
| 1 | 强制杀毒 | 外到内的数据，拷贝之前，自动完成强制杀毒、日志上报、数据交换全过程，杜绝数据交换过程中带来的病毒风险。 |
| 2 | 日志汇总 | 外网盘使用日志汇总 |
| 3 | 日志摆渡 | 外网盘使用日志，主机审计单机版日志，摆渡到内网服务器。摆渡过程在数据交换时进行，将外网盘日志同步到内网盘中， 当内网盘在内网中登录时自动上传日志到日志服务器 |
| 4 | 数据拷贝 | 数据不落地，内外网盘之间直接进行拷贝数据。 |
| 5 | 源盘及目的盘自动同步 | 需摆渡的文件存放在数据源安全U盘指定文件夹内进行自动同步  ▲需同时插入目的安全U盘，并输入两个U盘正确的密码，可选根据业务需要灵活选择内网盘到外网盘、外网盘到内网盘两种摆渡操作。（提供界面截图证明加盖原厂商公章） |
| 6 | 病毒查杀 | 任何有判定为有威胁的文档将会在查杀过程中被清除，不允许传送到目标安全U盘中；  ▲病毒无法清除的情况下则终止摆渡，若没有可调用的杀毒软件，则给出警告，但不停止摆渡过程提示是否继续进行摆渡。（提供界面截图证明加盖原厂商公章） |
| 7 | 日志同步 | 将外网盘缓存日志同步到内网盘。 |
| 8 | 文件摆渡 | 数据源安全U盘的“摆渡目录”文件夹下存放的文档将会在此次数据摆渡操作中传送到目标安全U盘。  若摆渡的目标安全U盘下存在“摆渡目录”，则此目录中包含的任何文档将会在摆渡数据时被删除。 |
|  | 安全可控U盘升级 | ▲需提供对安全U盘程序进行升级的功能，在U盘插入后检查程序版本，并根据需要提示升级。（提供界面截图证明加盖原厂商公章） |

### 中间机U盘注册管理系统功能参数要求

发盘工具部署在专用的国产化机器上；负责单位内数据安全交换系统专用安全移动存储介质的注册、管理，内网环境配置、日志服务器配置等

|  |  |  |
| --- | --- | --- |
| 序号 | **指标项** | **指标技术参数** |
| 1 | 登录密码 | 发盘工具需通过管理密码登录，并提供密码设置密码修改等功能 |
| 2 | 单位管理 | 对单位及部门信息进行增删改 |
| 3 | 用户管理 | 对用户信息进行增删改查  可手动条件用户信息到对应的部门  可批量导入导出用户信息 |
| 4 | 内外网环境判断条件设置 | 设置条件以便u盘程序判断是否在内网环境包含Windows及Linux系统下的条件；  1、▲Windows下包含服务器地址、进程名、注册表路径、注册表值、文件路径、文件包含字符串等判断条件。（提供界面截图证明加盖原厂商公章）  2、▲Linux下包含服务器地址、进程名、文件路径、文件包含字符串等判断条件。（提供界面截图证明加盖原厂商公章） |
| 5 | ▲日志服务器设置 | 可设置SysLog日志服务器的地址及端口。（提供界面截图证明加盖原厂商公章） |

### 原终端安全管理系统版本升级功能要求

|  |  |  |
| --- | --- | --- |
| **名称** | **指标项** | **指标技术参数** |
| 主机监控与审计系统功能 | 性能要求 | 支持win2000\2003\XP\Vista\WIN7\银河麒麟\中标麒麟等操作系统，集成主机桌面管理、操作系统和补丁管理、身份鉴别、电子文档管理、网络访问控制和系统可视化管理等十多类功能于一体。 |
| 管理用户分级 | 采用“三权分立”的用户管理权限：分别是系统管理员、安全保密管理员和安全审计员，可对各自不同的权限管理和日志管理等。 |
| ▲操作系统支持 | 支持国产操作系统中标麒麟、中科方德、银河麒麟满足国产化保密要求，提供证明材盖原厂盖章证明。 |
| 服务器自保护 | 当服务器通信端口负载超重时，服务器守护进程可自动重启服务器。 |
| 违规外联监控 | 防止对拨号设备（Modem，ADSL及无线网卡）或其他外联设备的使用，能够及时发现并阻止非法外联。能够对用户使用计算机上网或收发邮件等行为进行记录和报警，另外能够对网络端口进行监控，并控制聊天工具的使用。 |
| 非法接入监控 | 获取未安装客户端的非法主机，发出报警信息，采用分布式防护实时阻断非法主机的接入。 |
| 主机信息获取 | 系统能够自动获取终端的静态（IP地址、MAC地址、系统内存）和动态（设备使用情况、共享情况、拨号情况、主机帐号等）信息 |
| 身份认证 | 系统可基于CA的身份认证及权限管理，“用户名、口令+USB-KEY”双因子认证模式，对终端主机、服务器等本地、远程登录进行身份认证。 |
| 数据交换 | 外网和内网的数据交换通过中间机系统完成。 |
| 补丁分发 | 能够通过系统服务器端对系统内认证主机的操作系统的补丁自动分发。 |
| 外设管理 | 可全面监控并口、串口、软驱、光驱、PDA、1394、篮牙及SD卡等外设使用，并可定制特殊设备。 |
| 打印监控 | 监控受控主机上的打印情况，可以禁止、记录、允许用户提交打印任务，并且可以还原打印信息 |
| 主机性能监控 | 监控主机的CPU、磁盘、内存、网络带宽的占用率和网络连接数 |
| 移动存储介质安全交换模块 | ▲移动存储介质注册系统 | 系统提供外设可控U盘注册工具，可对移动存储介质（可控U盘）进行注册，注册后在系统内可以实现关联对的使用单位人员，进行统一管理及朔源。（提供界面截图证明加盖原厂商公章） |
| ▲移动存储介质使用记录审计 | 内置日志服务器，可接收移动存储介质（可控U盘）发送的syslog日志，进行关联分析至操作人员，审计U盘操作行为如插拔记录、增加删除文件、操作记录等。（提供界面截图证明加盖原厂商公章） |
| 其他 | ▲主机监控与审计系统产品证书 | 1）公安部《计算机信息系统安全专用产品销售许可证》（三级）  2）产品具有国家保密局《涉密信息系统产品检测证书》 |
| 售后服务 | 提供三年原厂服务 |

### 安全可控U盘技术参数要求

|  |  |
| --- | --- |
| **指标项** | **指标技术参数** |
| 安全可控U盘（外网版） | 配置120个专用安全U盘32G。防复制、防篡改、防病毒、防截屏录屏、防暴力破解、限时限次、文件隐藏等功能 |
| 硬件、固件、软件三者结合，实现全方位安全保障 |
| 加密文件系统自有高强度加密文件系统，支持大容量分区，支持大于4G的单个文件 |
| 防病毒传播私有加密文件系统，不提供通用的读写API。无论是否处于登录状态，非法进程都无法对盘进行读写。能自然避免病毒木马各种形式的自动复制执行 |
| ▲超限销毁;超出时间或次数限制的情况下，可以强制销毁盘内内容。内容销毁后，输入管理密码可以将盘恢复到出厂状态。提供界面截图证明加盖原厂商公章） |
| 提供移动存储介质审计功能，审计记录缓存于U盘闪存中。 |
| ▲防暴力破解密码、密码保护重试10次后，全盘强制自动销毁。（提供界面截图证明加盖原厂商公章） |
| 双密码模式具管理和访客两个模式，能够采用不同密码登录。登录界面无需输入用户类型。访客密码为空时，可自动登录访客模式。 |
| ▲电脑数量限制；识别电脑硬件信息，将盘绑定到指定数量的电脑，非绑定电脑上，访客禁止使用。（提供界面截图证明加盖原厂商公章） |
| ▲U盘管理系统提供Syslog接收服务器地址配置，可自定义IP地址和端口。（提供界面截图证明加盖原厂商公章） |
| 安全可控U盘（内网版） | 配置120个专用安全U盘32G。登陆认证、强制标记认证、安全审计、日志上次数据中心、支持Linux、Windows跨平台使用。 |
| 加密文件系统自有高强度加密文件系统，支持大容量分区，支持大于4G的单个文件 |
| 防病毒传播私有加密文件系统，不提供通用的读写API。无论是否处于登录状态，非法进程都无法对盘进行读写。能自然避免病毒木马各种形式的自动复制执行 |
| ▲超限销毁;超出时间或次数限制的情况下，可以强制销毁盘内内容。内容销毁后，输入管理密码可以将盘恢复到出厂状态。提供界面截图证明加盖原厂商公章） |
| 提供移动存储介质审计功能，审计记录缓存于U盘闪存中。 |
| ▲防暴力破解密码、密码保护重试10次后，全盘强制自动销毁。（提供界面截图证明加盖原厂商公章） |
| 双密码模式具管理和访客两个模式，能够采用不同密码登录。登录界面无需输入用户类型。访客密码为空时，可自动登录访客模式。 |
| ▲电脑数量限制；识别电脑硬件信息，将盘绑定到指定数量的电脑，非绑定电脑上，访客禁止使用。（提供界面截图证明加盖原厂商公章） |
| ▲U盘管理系统提供Syslog接收服务器地址配置，可自定义IP地址和端口。（提供界面截图证明加盖原厂商公章） |