高港区检察院杀毒软件及部署服务器设备项目询价通知书

本院就需要项目以询价方式组织采购。欢迎具有能力提供所要采购正品货物并且具备足够技术保障能力的供应商参加响应。

**一、项目概况**

1、询价采购编号：GGJCYXJ-201902

2、本项目采购预算：5.8万元。

**二、参加本次采购活动的供应商应当具备下列条件：**

符合《中华人民共和国政府采购法》第二十二条的有关规定：

（一）具有独立承担[民事责任](http://www.haosou.com/s?q=%E6%B0%91%E4%BA%8B%E8%B4%A3%E4%BB%BB&ie=utf-8&src=wenda_link)的能力；

（二）具有良好的商业信誉和健全的财务[会计制度](http://www.haosou.com/s?q=%E4%BC%9A%E8%AE%A1%E5%88%B6%E5%BA%A6&ie=utf-8&src=wenda_link)；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和[社会保障资金](http://www.haosou.com/s?q=%E7%A4%BE%E4%BC%9A%E4%BF%9D%E9%9A%9C%E8%B5%84%E9%87%91&ie=utf-8&src=wenda_link)的良好记录；

（五）参加[政府采购](http://www.haosou.com/s?q=%E6%94%BF%E5%BA%9C%E9%87%87%E8%B4%AD&ie=utf-8&src=wenda_link)活动前三年内，在经营活动中没有重大违法记录；

 （六）法律、[行政法规](http://www.haosou.com/s?q=%E8%A1%8C%E6%94%BF%E6%B3%95%E8%A7%84&ie=utf-8&src=wenda_link)规定的其他条件。

**三、采购内容（设备清单及参数要求）**

**1、杀毒软件部署服务器 1台 推荐品牌 曙光、浪潮、联想**

|  |  |
| --- | --- |
| 技术指标 | 招标参数 |
| 品牌要求 | 国内著名的国产服务器主流厂商。具备自主产品的研发、生产能力，设有国家重点实验室（提供证明） |
| 操作系统 | Windows 2012 |
| 机型 | 2U机架式服务器 |
| ★处理器 | 配置≥1颗XEON 4110 CPU |
| ★ 内存 | 配置≥16 GB DDR4 2666MHz ECC RDIMM内存 |
| ★ 硬盘 | 配置≥2块2TB 3.5吋7.2K 6Gb SATA硬盘； |
|  | 服务器硬盘6T企业级3.5寸SATA硬盘，2块; 服务器硬盘4T企业级3.5寸SATA硬盘，1块；服务器硬盘IBM,2.5寸，146GB10K SAS，2块；服务器硬盘IBM,2.5寸，600GB10K SAS，1块。 |
| 硬盘控制器 | 配置硬盘控制器，支持RAID0/1/10，支持电容掉电保护，支持后加电池 |
| ★网卡 | 板载双口千兆网卡， 支持NCSI、网络唤醒，网络冗余，负载均衡等网络高级特性 |
| ★扩展插槽 | 最大支持10个PCI-E 3.0插槽（2个内置专用插槽） |
| 电源 | 配置热插拔铂金1+1冗余电源，单个电源功率≥550W；提供服务器电源认证，并加盖原厂商公章； |
| 风扇 | 配置≥2个热插拔高速系统风扇 |
| 管理 | 集成BMC芯片，支持IPMI2.0和KVM Over IP高级管理功能 |
| ★服务 | 3年原厂整机质保，3年原厂免费上门服务（提供原厂项目授权函，原厂服务承诺函，原件） |
| 资质认证 | 通过3C认证、环标认证、节能认证，以上证书需要提供复印件并加盖厂家投标专用章  |
| ★安全可信 | 支持TPM安全可信模块，主机安全加固，支持操作系统安全加固模块，符合信息安全等级保护三级标准，提供自主知识产权软件注册权证书(加盖原厂商公章) |

**2、网络版杀毒软件1套（1个控制中心+5个服务器端+100个客户端，防病毒+补丁管理）推荐品牌：360网神、瑞星、微点**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 环境要求 | 控制中心安装环境要求 | 硬件环境：CPU至少4核以上；内存不低于4GB；硬盘不低于500GB，建议1T以上（需要下载补丁文件存放）； |
| 操作系统支持Windows Server 2008 R2/2012/2012 R2/2016的64位版本（简体中文版）；★要求支持CentOS 7、Redhat 7等Linux系统（要求Docker版本务必大于1.8.2）； |
| 要求支持在虚拟机上安装控制中心。 |
| Windows客户端安装环境要求 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10。 |
| 服务器客户端安装环境要求 | 要求支持操作系统:Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012；要求支持SUSE Linux/Red Hat Linux/CentOS/Ubuntu等操作系统。 |
| 系统管理 | 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能； |
| 客户端提供控制中心管理所需的相关数据信息，通讯可选择非明文方式；客户端执行最终的木马病毒查杀、漏洞修复等安全操作； |
| 要求支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行； |
| 要求支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理； |
| 要求支持控制中心迁移、数据备份、数据恢复。 |
| 资产管理 | 要求支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度； |
| 要求支持终端软、硬件变更审计，资产清单报表； |
| 要求支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率； |
| 要求支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件；**（要求提供产品界面截图并加盖厂家公章）** |
| ★要求支持正版软件的正版序列号的读取功能，确保软件正版化；**（要求提供产品界面截图并加盖厂家公章）** |
| 日志报表 | 要求支持展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况； |
| 要求支持展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况。 |
| 病毒、恶意代码、木马防护 | 内存防护 | 要求支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件。 |
| 启动防护 | 要求支持抢先加载防毒，在系统未加载前启动文件监控，通常情况下不必重启到安全模式也能清除病毒。 |
| 注册表、引导区防护 | 要求支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀。 |
| 电子邮件防护 | 要求支持电子邮件内文件检测，可清除隐藏于电子邮件计算机病毒和恶性程序。 |
| 网页安全防护 | 要求能够对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页挂马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息。 |
| 网络安全防护 | 要求支持拦截下载器自动下载木马程序、恶意推广程序、盗号木马；要求支持拦截黑客远程控制本机。 |
| 嵌入式防御 | 要求支持用户添加嵌入杀毒的应用程序；支持FlashGet、NetAnts、WinZip、WellGet、WinRAR等工具的嵌入式杀毒功能。 |
| 移动设备病毒防护 | 要求提供U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马。 |
| 局域网共享查杀 | 要求能够对局域网共享文件传输进行检测和查杀。 |
| 浏览器防护 | 要求支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置。 |
| 文件传输防护 | 要求支持U盘等移动磁盘设备和电脑硬盘间文件传输检测；要求支持局域网共享文件传输检测。 |
| 攻击防护 | 要求能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质、创建系统账号。 |
| ★云修复 | 要求支持扫描发现文件遭破坏或被感染时触发修复流程，修复通过公有云下载正常文件替换遭破坏的文件。**（要求提供产品界面截图并加盖厂家公章）** |
| 黑白名单例外 | 要求支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件；要求支持手工导入MD5+SHA1的黑白名单方式，支持txt批量导入方式；要求支持文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件；要求支持下发忽略白名单的病毒扫描；要求支持对windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理。 |
| 病毒查杀统计 | 要求支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件； |
| 要求支持按病毒、木马、终端等维度统计全网病毒感染状况； |
| 要求上报文件至少包括:文件名称、发现时间、鉴定结果、文件大小、数字签名和文件所属源计算机等信息。 |
| 漏洞利用防御 | 要求能够支持XP系统的漏洞利用防御，尤其对通过文件漏洞的攻击行为进行有效检测与防御。 |
| 压缩包杀毒 | 要求支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力；要求支持可对压缩包层级设置以节省终端计算资源。 |
| 备份区隔离区管理 | 要求可对备份区、隔离区的文件进行有效管理。能够对单个、指定的文件和全部文件，进行文件的删除、恢复等多项管理措施。 |
| 敲诈者病毒防御 | ★要求对敲诈者病毒提供专有的防护功能；**（要求提供产品界面截图并加盖厂家公章）** |
| 私有云引擎 | 要求产品具备公有云与本地私有云检测能力。 |
| 要求支持部署私有云查杀引擎，增强本地隔离网查杀效果。 |
| 样本库数量 | 要求产品具备公有云检测能力，并且公有云特征储备超过145亿。 |
| 要求支持私有云查杀，预置至少8亿黑名单及2亿白名单，终端威胁统一到控制中心查询黑白并进行查杀。 |
| 补丁分发与漏洞修复 | 要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型； |
| 要求支持漏洞修复影响文档编辑时提醒功能； |
| 要求支持补丁下载安装顺序设置，可以有效节省漏洞修复时间与减少CPU占用； |
| 要求支持终端智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁； |
| 要求产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能。 |
| 其他系统的支持要求 | 要求至少支持Windows Server 2003、2008、2012 三个版本操作系统平台的杀毒防护与漏洞管理，并可对Windows xp 和Windows Server 2003提供后续漏洞防护； |
| 要求支持苹果MAC OS X系统的病毒防护功能。 |
| 扩展功能支持要求 | ★要求本系统支持如下扩展功能：运维管控、移动存储介质管理、XP防护、终端审计、终端综合评估、终端准入控制、软件管家/软件分发。**要求提供厂家盖章的承诺函原件。** |
| 产品资质要求（提供相关复印件，并加盖厂家公章） | ★要求提供公安部颁发的《计算机信息系统安全专用产品销售许可证》内网主机监测（一级）资质证书；要求提供相关的《计算机软件著作权登记证书》资质证书；要求具备病毒查杀引擎系统的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书；★要求提供全球IPv6 Ready测试中心出具的认证证书；★要求具备网络安全准入系统的销售许可证，提供公安部颁发的《计算机信息系统安全专用产品销售许可证》终端接入控制（一级）资质证书；★要求提供公安部颁发的《计算机信息系统安全专用产品销售许可证》USB移动存储介质管理系统（一级）资质证书。 |
| 厂商资质要求（提供相关复印件，并加盖厂家公章） | 要求厂家为CNCERT网络安全应急服务支撑单位（具备国家级级别）；要求厂家具备中国信息安全认证中心《信息安全服务资质证书》（一级应急处理服务资质）。 |
| 配置要求 | ★本次要求配置**100**个计算机客户端+**5**个windows服务器，软件功能具备“防病毒+补丁管理”，并管理控制中心的客户名称为“泰州市高港区人民检察院”。 |
| 保修和服务 | ★要求提供原厂三年升级质保服务承诺函原件。 |
| 厂家项目授权书 | ★要求提供针对本项目的厂家授权书原件。 |

**四、采购内容的质量、技术和服务等要求**

1、技术要求

（1）所有报价产品的生产、制造、安装等，各项技术标准应当符合国家（强制性）标准、国家没有相应标准、规范的，可使用行业标准、规定；非标设备按采购文件约定的技术要求和规范。

（2）响应产品是全新的、未使用过的、原包装未拆封的商品，完全符合采购要求规定的质量、规格和性能的要求，响应单位应保证其提供的产品在正确安装、正常使用和保养条件下，在规定的使用寿命期内具有满意的性能。

（3）供应商响应的产品必须明确具体的品牌规格型号及参数且必须达到上述的技术指标，技术参数不得负偏离。

2、交货及验收

（1）交货地点：高港区检察院；

（2）采购货物的交货时间：自采购合同签订之日起7日内交货并完成安装调试，如不能如期供货，采购单位有权终止合同，成交单位须承担由此对采购方造成的损失；

（3）采购货物的验收：

①产品配置必须原厂出厂时全部自带，所有设备外包装箱不得自行拆封，包装箱上所有标签等不得涂改或撕毁，否则采购单位有权拒绝验收。所有货物交货完毕，采购人及采购人指定部门对成交单位提供的产品进行检测，检测不符合采购要求的，采购人有权终止合同，没收成交单位提供的所有产品。相关损失由成交单位自行承担。响应报价时应充分考虑该费用，采购单位不再另行支付。

②符合设备本身的规格、技术条件及乙方承诺的其它指标；

③采购货物的验收时间：货到安装调试完成后3个工作日；

3、售后服务要求：

3.1、免费质保期按不低于采购内容表格内要求执行，终身服务。其他未注明的按国家、厂商、行业标准孰优执行，质保期由设备验收合格后开始计算。询价响应单位必须在询价响应文件中注明所响应产品的免费质保期，否则为无效询价响应文件。

3.2质量保证期内，如果证实货物是有缺陷的，包括潜在的缺陷或者使用不符合要求的材料等，成交供应商应立即免费维修或者更换有缺陷的货物或者部件，保证达到合同规定的技术以及性能要求。如果成交供应商在收到通知后 五 天内没有弥补缺陷，采购人可自行采取必要的补救措施，但风险和费用由成交供应商承担，采购人同时保留通过法律途径进行索赔的权利。

3.3、售后服务：供应商应提供及时周到的售后服务，保证至少一次上门回访、检修。在接采购人通知 1 小时做出响应， 4 小时内到达现场， 8 小时内维修完毕，不能在规定时间内修好的2天内要免费提供备品（机）备件。

3.4、成交供应商免费为采购人提供中文操作手册并培训操作人员，其中包括讲解产品的结构以及原理、产品的使用以及维护保养，直至操作人员能够独立的操作使用。

4、采购合同的签订：在成交通知书发出之日起3天内与采购方签订采购合同，否则将视为完全自愿放弃关于本次采购的成交人资格，并承担所有因此而对采购方造成的损失。

**五、响应报价要求**

1、报价响应包括上述货物、配件、运输、管理、维护、保险、利润、税金、现场安装(调试达到正常可使用状态)、培训、政策性文件规定及合同包含的所有风险、责任等各项应有费用。

2、响应时可以对采购报价应采购标段内所要采购的全部内容全部进行报价，只响应其中部分内容或出现选择性报价者，其报价将被拒绝。总体报价在符合设备清单及参数要求的基础上，最低价中标。

**六、采购货物的付款方式**

合同生效后标的物须在合同规定的时间内全部运送到交货地点、安装调试完毕，经验收合格后支付一次性付清。

货款结算时，需提供以下资料：

A、验收报告。

B、合格销售发票。

C、由供需双方签章的《采购合同》。

**七、询价响应方式**

（一）、响应文件的递交

1、询价响应文件递交截止时间：2019年11月18日上午9：00前，将响应文件密封送达指定地点。过时送达的响应文件将被拒绝。

询价响应文件递交地点：高港区检察院301办公室

2、询价响应的评审时间和地点：本项目于2019年11月18日上午9:00时在高港区检察院302会议室确定成交单位。

（二）、响应文件的制作要求：

 1、响应文件的组成：

（1）有效的工商营业执照（副本）、税务登记证（副本）；

（2）询价响应单位法定代表人（负责人）身份证复印件；

 （3）报价货物的品牌、规格、参数、性能等说明；

（4）售中、售后服务承诺（包括免费质保期承诺、交货期说明等）；

 （5）报价货物的销售代理资质、授权等（若有）；

 （6）《询价响应报价明细表》；

 （7）《询价响应承诺书》

 2、文件的签署和密封要求：

 （1）按上述要求制作询价响应文件正本壹本；

 （2）询价响应文件须装袋密封，封口处须加盖单位公章，密封袋及相应文件封面上应注明采购项目名称、采购编号、标段号、响应单位名称、地址、联系人、联系电话等。

（三）、响应文件错误的修正原则

 1、响应文件的大写金额与小写金额不一致的，以大写金额为准。总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；单价金额小数点有明细错位的，应以总价为准，并修改单价；

 2、对不同文字文本投标文件的解释发生异议的，以中文文本为准。

 3、供应商不同意以上修正的，其询价响应文件将被拒绝。

（四）、响应文件的补充、修改和撤回

供应商在提交询价响应文件截止时间前，可以对所提交的响应文件进行补充、修改或者撤回，并书面通知采购代理机构。补充、修改的内容作为响应文件的组成部分。补充、修改的内容与响应文件不一致的，以补充、修改的内容为准。

**八、项目的终止**

 出现下列情形之一的，将终止询价采购活动：

 1、因情况变化，不再符合规定的询价采购方式适用情形的；

 2、出现影响采购公正的违法、违规行为的；

 3、在采购过程中符合竞争要求的供应商或者报价未超过采购预算的供应商不足3家的。

**九、联系及监督**

 采购单位：高港区人民检察院

 联 系 人：汪先生 联系电话： 0523-86960181

 附件下载：高港区检察院杀毒软件及部署服务器设备项目询价通知书

泰州市高港区人民检察院

2019年11月12日