**杭州市临安区机房信息数据安全保护设备采购建设项目公开招标文件**

 （项目编号LZC-GK-2020-11161）

采购单位：杭州市临安区数据资源管理局

采购机构：杭州市公共资源交易中心临安分中心

备案单位：杭州市临安区政府采购办公室

地 址：杭州市临安区行政服务中心B座四楼

**目 录**

1. 采购公告
2. 投标须知
3. 评标办法及评标标准

第四章 采购需求

第五章 政府采购合同主要条款

第六章 投标文件格式

**第一章 采购公告**

受杭州市临安区数据资源管理局的委托，杭州市公共资源交易中心临安分中心（以下简称“采购机构”），就以下杭州市临安区机房信息数据安全保护设备采购建设项目进行公开采购，现欢迎有供货能力的合格供应商参加投标。

一、**项目编号：**LZC-GK-2020-11161

**二、采购内容及数量**

|  |  |  |  |
| --- | --- | --- | --- |
| 项目名称 | 数量 | 技术要求 | 上限价 |
| 杭州市临安区机房信息数据安全保护设备采购建设项目 | 1 | 详见采购需求 | 146万元 |

**三**、**合格供应商资格要求**

1.符合《中华人民共和国政府采购法》第二十二条之规定；

2.未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）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；

3.不允许联合体投标。

**四、投标报名**

**本项目实行网上报名，不接受现场报名。投标截止时间前，供应商自行登录浙江政府采购网（**[http://zfcg.czt.zj.gov.cn](http://zfcg.czt.zj.gov.cn/)**）进行报名。**

**《供应商网上报名操作指南》网址：浙江政府采购网，位置：“首页-办事指南-省采中心-网上报名”（**http://zfcg.czt.zj.gov.cn/bs\_other/2018-03-30/12002.html?\_=2020-08-17%2003:00:46**）。**

**五、采购文件的获取**：

自本公告发布之日起在公告附件中免费下载，下载地址：

浙江政府采购网：（[http://zfcg.czt.zj.gov.cn](http://zfcg.czt.zj.gov.cn/)）；

杭州市公共资源交易网：（<https://www.hzctc.cn/Index/Home>）；

临安区政府采购网：(<http://www.linan.gov.cn/col/col1366369/>)

**（注：采购公告上附件里的采购文件仅供阅览使用，报名成功后才视作供应商依法获取采购文件，未进行报名的供应商，对采购文件提起的质疑，将不予受理。）**

**六、投标保证金**：无

**七、投标说明**

**1.本项目实行电子投标，投标人无须提交纸质投标文件，无须授权代表参加开标会议。应按照本项目招标文件和政采云平台的要求编制、加密并递交投标文件。供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题，可致电政采云平台技术支持热线咨询，联系方式：400-881-7190。**

**2.投标人应在开标前完成CA数字证书办理。（办理流程详见<http://www.zjzfcg.gov.cn/bidClientTemplate/2019-05-27/12945.html>）。完成CA数字证书办理预计一周左右，建议各投标人抓紧时间办理。**

**3.投标人通过“政采云”平台电子投标工具制作投标文件，电子投标工具请供应商自行前往浙江省政府采购网下载并安装，（下载网址：<http://www.zjzfcg.gov.cn/bidClientTemplate/2019-05-27/12946.html>），电子投标具体流程详见本招标公告附件：“[政采云供应商项目采购-电子招投标操作指南.pdf](file:///C%3A%5C%5CUsers%5C%5CAdministrator%5C%5CDocuments%5C%5CWeChat%20Files%5C%5Cw830616%5C%5CFileStorage%5C%5CFile%5C%5CDocuments%5C%5CWeChat%20Files%5C%5Cw830616%5C%5CFileStorage%5C%5CGao%5C%5CDocuments%5C%5CWeChat%20Files%5C%5Chawer122%5C%5CFileStorage%5C%5CFile%5C%5C2019-06%5C%5C%E7%94%B5%E5%AD%90%E5%8C%96%E6%8A%95%E6%A0%87%E6%93%8D%E4%BD%9C%E6%8C%87%E5%8D%97.pdf)”。**

**八、投标截止时间和地点**：

**本项目于2021年1月20日9:00投标截止。**

投标人应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标、响应截止时间后送达的投标、响应文件，将被政采云平台拒收。

**九、业务咨询：**

杭州市公共资源交易中心临安分中心 联系人：胡旭晨

联系电话：0571-23616011 传真：0571-23616016

质疑答复岗联系人：张晨 联系电话：0571-23616016

采购单位联系人：方忠平 联系电话：0571-63700016

 杭州市公共资源交易中心临安分中心

 2020年12月15日

**第二章 投标须知**

|  |  |
| --- | --- |
| 序号 | 内 容 及 要 求 |
| 1 | 项目名称：杭州市临安区机房信息数据安全保护设备采购建设项目 |
| 2 | 投标保证金应按《采购公告》六规定交纳。 |
| 3 | 答疑与澄清：投标供应商如认为招标文件表述不清晰、存在歧视性或者其他违法内容的，应当以书面形式要求采购机构或采购人作出书面解释、澄清或者向采购机构提出书面质疑，逾期不再受理。 |
| 4 | 投标截止时间：2021年1月20日9时00分 |
| 5 | 开标时间、地点：2021年1月20日9时00分.本项目采用全流程电子化交易，无须参加现场开标 |
| 6 | **本项目实行网上投标。目前政府采购全流程电子化交易，供应商应准备电子投标文件，按政采云平台项目采购-电子招投标操作指南及本招标文件要求递交。投标文件均由资质文件、技术及商务文件、报价文件组成。投标人务必按时自行解密，规定时间内解密失败者作无效响应处理。** |
| 7 | **投标文件的接受：投标人应当在投标截止时间前完成电子投标文件的传输递交，并可以补充、修改或者撤回电子投标文件。补充或者修改电子投标文件的，应当先行撤回原文件，补充、修改后重新传输递交。投标截止时间前未完成传输的，视为撤回投标文件。投标、响应截止时间后送达的投标、响应文件，将被政采云平台拒收。投标人还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份。备份投标文的制作、存储、密封详见招标文件第二章第二部分“投标文件的编制”第八点“备份投标文件”。** |
| 8 | 评审结果公示：评审结束后两个工作日内，中标公示于浙江省政府采购网、杭州市公共资源交易网，公示无异议后发出中标通知书。 |
| 9 | 签订合同时间：中标通知书发出后30日内。 |
| 10 | 付款方式：国库集中支付（采购人自行支付），详见采购需求。 |
| 11 | 信用记录：根据财库[2016]125号文件，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn），以开标当日网页查询记录为准。对列入失信被执行人、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的供应商，其投标将作无效标处理。 |
| 12 | 政府采购节能环保产品：投标产品若属于节能环保产品的，请提供财政部、环境保护保部发布有效期内环境标志产品政府采购清单以及财政部、发改委联合发布有效期内节能产品政府采购清单。招标需求中要求提供的产品属于节能清单中政府强制采购节能产品品目的，投标人须提供该清单内产品，否则其投标将作为无效标处理。 |
| 13 | 小微企业有关政策：1、根据财库〔2011〕181号和《关于优化营商环境进一步加强政府采购监督管理工作的通知》杭财采监〔2020〕7号的相关规定，在评审时对小型和微型企业的投标报价给予10%的扣除（专门面向中小企业的项目，对小微企业给予8%的价格扣除），用扣除后的价格参与评审。属于小型和微型企业的，投标文件中投标人必须提供的《中小企业声明函》以及本单位、制造商（如有）“国家企业信用信息公示系统——小微企业名录”页面查询结果（查询时间为投标前一周内，并加盖本单位公章），并在报价明细表中说明制造商情况。联合体投标时，联合体各方均为小型、微型企业的，联合体视同为小型、微型企业享受政策;联合体其中一方为小型、微型企业的，联合协议中约定小型、微型企业的协议合同金额占到联合体协议合同总额30%以上的，给予联合体 (2-3%)的价格扣除，须同时提供联合体协议约定（包含小型、微型企业的协议合同份额）。2、根据财库[2017]141号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库[2017]141号文件第一条的规定，并在投标文件中提供残疾人福利性单位声明函（见附件）。3、根据财库[2014]68号的相关规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除政策，并在投标文件中提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件（格式自拟）。(注：未提供以上材料的，均不给予价格扣除）。4、凡已在浙江政府采购网网上注册入库，并取得临安区政府采购合同的中小企业供应商，均可申请政府采购信用融资，联系方式见附表（政府采购融资畅通工程金融机构联系信息表）。 |
| 14 | 投标文件有效期：90天 |
| 15 | 解释：本采购文件的解释权属于杭州市公共资源交易中心临安分中心。 |

**一、总 则**

（一）适用范围

仅适用于本次采购文件中采购项目的投标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

（二）定义

1.“采购机构”系指组织本次采购的杭州市公共资源交易中心临安分中心。

2.“投标人”系指向采购机构提交投标文件的单位。

3.“采购人” 系指委托采购机构采购本次项目的国家机关、事业单位和团体组织。

4.“产品”系指供方按采购文件规定，须向采购人提供的一切设备、保险、税金、备品备件、工具、手册及其它有关技术资料和材料。

5.“服务”系指采购文件规定供方须承担的安装、调试、技术协助、校准、培训、技术指导以及其他类似的义务。

6.“项目”系指投标人按采购文件规定向采购人提供的产品和服务。

（三）开标委托

全权代表须携带有效身份证件。如全权代表不是法定代表人，须有法定代表人出具的授权委托书（正本用原件，副本可用复印件并加盖公章，格式见第六部分）。

（四）投标费用

不论采购结果如何，投标人均应自行承担所有与投标有关的全部费用（采购文件有其他规定的除外）。

（五）特别说明：

1.投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有。投标人投标所使用的采购项目实施人员必须为本法人员工（或必须为本法人或控股公司正式员工）。

2. 投标人应仔细阅读采购文件的所有内容，按照采购文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

（六）质疑

质疑应当采用加盖投标人公章的书面形式，质疑书应明确阐述采购过程或成交结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理，否则，采购机构将不予受理。

（七）采购文件的澄清与修改

1. 投标人应认真阅读本采购文件，发现其中有误或有不合理要求的，投标人应当以书面形式向杭州市公共资源交易中心临安分中心提出。交易中心将在规定的时间内，在财政部门指定的政府采购信息发布媒体上发布更正公告。

2.采购文件澄清、答复、修改、补充的内容为采购文件的组成部分。当采购文件与采购文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

**二、投标文件的编制**

**（一）投标文件的形式**

**投标文件分为电子投标文件。电子投标文件，按“政采云供应商项目采购-电子招投标操作指南”及本招标文件要求制作、加密并递交。**

**（二）投标文件的组成**

**投标文件组成均为资格文件、技术及商务文件、投标报价文件三部份组成。其中电子投标文件中所须加盖公章部分均采用CA签章。**

**1.资格文件（不含报价）：**

（1）投标声明书 (格式见附件，含重大违法记录声明)；

（2）提供自招标公告发布之日起至投标截止日内任意时间的“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）投标人信用查询网页截图。（以开标当日采购人或由采购人委托的评标委员会核实的查询结果为准）

（3）法定代表人授权委托书(格式见附件)；

（4）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

（5）提供有效的依法缴纳税收证明（完税凭证或税务部门出具的证明）；

（6）提供有效的依法缴纳社会保障资金证明（缴纳凭证或人社部门出具的证明）；

（7）2019年度资产负债表等财务报表资料文件 (或其它财务状况报告，新成立的公司，必须提供情况说明)；

（8）联合投标协议书（若需要）;

（9）联合投标授权委托书（若需要）;

（10）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

**注：以上目录是编制资信及商务内容的基本格式要求，投标人可根据自身情况进一步细化。**

**2.技术及商务文件（不含报价）：**

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人力资源安排、项目组人员清单等）（格式见附件）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）（格式见附件）；

（12）投标方认为需要的其他文件资料。

**注：以上目录是编制技术响应内容的基本格式要求，供参考，投标人可根据自身情况进一步补充、细化、优化。**

**3.报价文件：**

（1）开标一览表（报价表）

（2）报价明细清单

（3）小微企业声明函及相关资料、残疾人福利性单位相关资料（如有）

（4）采购文件要求的或投标人认为需要的其它资料

**4.资格后审等所需原件包括下列内容：（若有）**

采购文件要求提供原件的材料。

为便于专家评标：a、以上资格后审、资信评审而要求投标人提供企业资料原件的，投标人应另袋单独密封包装在一个袋内；b、以上原件采购文件若要求提供复印件的仍需将复印件装订进投标响应文件。

**（三）投标文件的语言及计量**

1.投标文件以及投标人与采购机构就有关投标事宜的所有来往函电，均应以中文汉语书写。除签名、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的投标文件视同未提供。

2.投标计量单位，采购文件已有明确规定的，使用采购文件规定的计量单位，采购文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），否则视同未响应。

**（四）投标报价**

1.投标文件只允许有一个报价，报价应按采购文件中相关附表格式填报

2.投标报价是履行合同的最终价格，应包括货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修等一切税金和费用。

**（五）投标文件的有效期**

1.自投标截止日起90天内投标文件应保持有效。有效期不足的投标文件将被拒绝。

2.成交供应商的投标文件自开标之日起至合同履行完毕止均应保持有效。

**（六）投标保证金（若有）**

1.投标人须按规定提交投标保证金。

2.保证金形式：汇票、电汇、支票等非现金方式。

3.保证金不计息。

4.投标保证金的交付时间以专户实际收到交纳资金为准。

5.投标人在交纳投标保证金时，需在进账凭证上注明用途和项目编号，以便查实核对。

6. 投标人有下列情形之一的，投标保证金将不予退还：

（1）投标人在投标截止时间后撤回投标文件的

（2）投标人在投标过程中弄虚作假，提供虚假材料的

（3）投标人无故放弃或无正当理由不与采购人签订合同的

（4）将中标项目转让给他人或者在投标文件中未说明且未经采购单位同意，将中标项目分包给他人的

（5）未按规定提交履约保证金的

（6）其他严重扰乱招投标程序的

7.投标保证金的退还：未成交人投标保证金在成交通知书发出后5个工作日内退还。成交人的投标保证金在合同签订后5个工作日内凭鉴证合同退还。

**（七）投标文件的签署和份数**

**投标人应根据“政采云供应商项目采购-电子招投标操作指南”及本招标文件规定的格式和顺序编制电子投标文件并进行关联定位。**

1. **备份投标文件**

1投标人在电子交易平台传输递交投标文件后，还可以在投标截止时间前直接提交或者以邮政快递方式递交备份投标文件1份，**但采购人、采购机构不强制或变相强制投标人提交备份投标文件。**

2备份投标文件须在“政采云投标客户端”制作生成，并储存在DVD光盘中。备份投标文件应当密封包装并在包装上加盖公章并注明投标项目名称，投标人名称**▲不符合上述制作、存储、密封规定的备份投标文件将被视为无效或者被拒绝接收。**

3直接提交备份投标文件的，投标人应于投标截止时间前在招标公告中载明的开标地点将备份投标文件提交给采购机构，采购机构将拒绝接受逾期送达的备份投标文件。

4以邮政快递方式递交备份投标文件的，投标人应先将备份投标文件按要求密封和标记，再进行邮政快递包装后邮寄。备份投标文件须在投标截止时间之前送达浙江省杭州市临安区锦北街道科技大道4398号B座4楼B448办公室；送达时间以签收人签收时间为准（签收人：杨颖， 联系电话：18768193991）。采购机构将拒绝接受逾期送达的备份投标文件。邮寄过程中，电子备份投标文件发生泄露、遗失、损坏或延期送达等情况的，由投标人自行负责。

**5投标人仅提交备份投标文件，没有在电子交易平台传输递交投标文件的，投标无效。**

**三、开标**

**（一）组织开标程序**

招标方将按照招标文件规定的时间、地点和程序组织开标，各投标人无须参加现场开标会议，请自行登录政采云平台关注开标信息。

1.开标会由招标方主持，主持人介绍开标现场的人员情况，宣读递交投标文件的投标人名单、开标纪律、应当回避的情形等注意事项。

**2.电子招投标开标及评审程序**

**2.1投标截止时间后，投标人登录政采云平台，用“项目采购-开标评标”功能对电子投标文件进行在线解密。在线解密电子投标文件时间为开标时间起半个小时内。投标文件未按时解密，投标人提供了备份投标文件的，以备份投标文件作为依据，否则视为投标文件撤回。投标文件已按时解密的，备份投标文件自动失效。**

**2.2.评标委员会对资格和商务技术响应文件进行评审；**

**2.3在系统上公开资格和商务技术评审结果；**

**2.4在系统上公开报价开标情况；**

**2.5评标委员会对报价情况进行评审；**

**2.6在系统上公布评审结果。**

**特别说明：1、政采云公司如对电子化开标及评审程序有调整的，按调整后的程序操作。**

**2、目前政府采购全流程电子化交易，投标人须在规定时间内自行解密。**

**3.本项目原则上采用政采云电子招投标开标及评审程序，但有下情形之一的，按以下情况处理：**

**3.1若个别投标人在规定时间内无法解密或解密失败的作无效投标处理。解密成功的投标人不足三家的，本项目流标重新组织采购活动。**

**3.2若因政采云平台原因无法读取或电子开评标无法正常进行，交易中心将情况上报行业监管部门同意后，重新组织采购活动。**

**（二）组织评标程序**

招标方将按照招标文件规定的时间、地点和程序组织评标，各评审专家及相关人员应参加评审活动并接受核验、签到，无关人员不得进入评审现场。

1.按规定统一收缴、保存评标现场相关人员通讯工具。

2.介绍评审现场的人员情况，宣布评审工作纪律，告知评审人员应当回避情形；组织推选评标委员会组长。

3.宣读提交投标文件的供应商名单，组织评标委员会各位成员签订《政府采购评审人员廉洁自律承诺书》。

4.采购人可以在评标前说明项目背景和采购需求，说明内容不得含有歧视性、倾向性意见，不得超出招标文件所述范围。说明应当提交书面材料，并随采购文件一并存档。

5.根据需要简要介绍招标文件（含补充文件）制定及质疑答复情况、按书面陈述项目基本情况及评审工作需注意事项等，让评审专家尽快知悉和了解所评审项目的采购需求、评审依据、评审标准、工作程序等；提醒评标委员会对客观评审项目应统一评审依据和评审标准，对主观评审项目应确定大致的评审要求和评审尺度；对评审人员提出的有关招标文件、投标文件的问题进行必要的说明、解释或讨论。

6.采购人代表或由采购人委托的评标委员会对投标人资格文件进行审查并以开标当日为准对投标人“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）信用记录情况进行核实，资格不符合的，应组织相关投标人代表进行陈述、澄清或申辩。

7.评标委员会组长组织评审人员独立评审。评标委员会对拟认定为投标文件无效，应组织相关投标人代表进行陈述、澄清或申辩；招标方可协助评标委员会组长对打分结果进行校对、核对并汇总统计；对明显畸高、畸低的评分（其总评分偏离平均分30%以上的），评标委员会组长应提醒相关评审人员进行复核或书面说明理由，评审人员拒绝说明的，由现场监督员据实记录；评审人员的评审、修改记录应保留原件，随项目其他资料一并存档。

8.做好评审现场相关记录，协助评标委员会组长做好评审报告起草、有关内容电脑文字录入等工作，并要求评标委员会各成员签字确认。

9.评审结束后，招标方应对评标委员会各成员的专业水平、职业道德、遵纪守法等情况进行评价；同时按规定向评审专家发放评审费，并交还评审人员及其他现场相关人员的通讯工具。

**（三）评审程序**

1.在评审专家中推选评标委员会组长。

2.评标委员会组长召集成员认真阅读招标文件以及相关补充、质疑、答复文件、项目书面说明等材料，熟悉采购项目的基本概况，采购项目的质量要求、数量、主要技术标准或服务需求，采购合同主要条款，投标文件无效情形，评审方法、评审依据、评审标准等。

3.评审人员对各投标人投标文件的有效性、符合性、完整性和响应程度进行审查，确定是否对招标文件作出实质性响应。

4.评审人员按招标文件规定的评审方法和评审标准，依法独立对投标人投标文件进行评估、比较，并给予评价或打分，不受任何单位和个人的干预。

5.评审人员对各供应商投标文件非实质性内容有疑议或异议，或者审查发现明显的文字或计算错误等，及时向评标委员会组长提出。经评标委员会商议认为需要供应商作出必要澄清或说明的，应通知该投标人以书面形式作出澄清或说明。授权代表未到场或拒绝澄清说明或澄清说明的内容改变了投标文件的实质性内容的，评标委员会有权对该投标文件作出不利于投标人的评判。书面通知及澄清说明文件应作为政府采购项目档案归档留存。

6.评审人员需对招标方工作人员唱票或统计的评审结果进行确认，现场监督员应对评审结果签署监督意见。如发现分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致以及存在评分畸高、畸低情形的，应由相关人员当场改正或作出说明；拒不改正又不作说明的，由现场监督员如实记载后存入项目档案资料。

7.评标委员会根据评审汇总情况和招标文件规定确定中标候选供应商排序名单。

8.起草评审报告，所有评审人员须在评审报告上签字确认。

**（四）评审原则**

1.评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。

2.评审专家因回避、临时缺席或健康原因等特殊情况不能继续参加评审工作的，应按规定更换评审专家,被更换的评审人员之前所作出的评审意见不再予以采纳，由更换后的评审人员重新进行评审。无法及时更换专家的，要立即停止评审工作、封存评审资料，并告知投标人择期重新评审的时间和地点。

3.评审人员对有关招标文件、投标文件、样品或现场演示（如有）的说明、解释、要求、标准存在不同意见的，持不同意见的评审人员及其意见或理由应予以完整记录，并在评审过程中按照少数服从多数的原则表决执行。对招标文件本身不明确或存在歧义、矛盾的内容，应作对投标人而非采购人有利的解释；对因招标文件中有关产品技术参数需求表述不清导致投标人实质性响应不一致时，应终止评审，重新组织采购。评审人员拒绝在评审报告中签字又不说明其不同意见或理由的，由现场监督员记录在案后，可视为同意评审结果。

**4.财政部令第87号《政府采购货物和服务招标投标管理办法》第三十一条规定：使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。**

**非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前款规定处理。**

**四、评标**

**详见第三章评标办法及评标标准**

**五、定标**

（一）确定成交人。本项目由采购人确定成交人。

1.评标结束，评审报告经采购人确认后，将采购结果发布采购公告的网站上，进行7个工作日的预成交公示。

2.采购人对评标结果无异议的，采购人应在收到评标报告后5个工作日内对评标结果进行确认。如有投标人对评标结果提出质疑的，采购人可在质疑处理完毕后确定成交人。

（二）采购人依法确定成交人后，采购机构以书面形式发出《成交通知书》。

（三）质疑和投诉：各参加政府采购活动的供应商认为本采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、采购代理机构提出质疑。质疑供应商对采购人、采购代理机构的答复不满意，或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。质疑函范本、投诉书范本请到浙江政府采购网下载专区下载。

**六、****合同授予**

（一）签订合同

1.成交人应自成交通知书发出后30日内与采购人签定合同。

2.成交人拖延、拒签合同的,将被扣罚投标保证金并取消成交资格。

（二）履约保证金

详见第四章采购需求。

**七、货款的结算**

详见第四章采购需求。

**八、其它**

▲《中华人民共和国政府采购法》第七十七条 供应商有下列情形之一的，处以采购金额千分之五以上千分之十以下的罚款，列入[不良行为记录](http://baike.baidu.com/view/2183629.htm%22%20%5Ct%20%22_blank)名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由[工商行政管理机关](http://baike.baidu.com/view/2292396.htm%22%20%5Ct%20%22_blank)吊销营业执照；构成犯罪的，依法追究刑事责任：

（一）提供虚假材料谋取中标、成交的；

（二）采取不正当手段诋毁、排挤其他供应商的；

（三）与采购人、其他供应商或者采购代理机构恶意串通的；

（四）向采购人、采购代理机构行贿或者提供其他不正当利益的；

（五）在招标采购过程中与采购人进行协商投标的；

（六）拒绝有关部门监督检查或者提供虚假情况的。

供应商有前款第（一）至（五）项情形之一的，中标、成交无效。

▲《中华人民共和国政府采购法实施条例》第七十二条　供应商有下列情形之一的，依照政府采购法第七十七条第一款的规定追究法律责任：

　　（一）向评标委员会、竞争性投标小组或者询价小组成员行贿或者提供其他不正当利益；

　　（二）中标或者成交后无正当理由拒不与采购人签订政府采购合同；

　　（三）未按照采购文件确定的事项签订政府采购合同；

　　（四）将政府采购合同转包；

　　（五）提供假冒伪劣产品；

　　（六）擅自变更、中止或者终止政府采购合同。

　　供应商有前款第一项规定情形的，中标、成交无效。评审阶段资格发生变化，供应商未依照本条例第二十一条的规定通知采购人和采购代理机构的，处以采购金额5‰的罚款，列入不良行为记录名单，中标、成交无效。

　　▲《中华人民共和国政府采购法实施条例》第七十三条　供应商捏造事实、提供虚假材料或者以非法手段取得证明材料进行投诉的，由财政部门列入不良行为记录名单，禁止其1至3年内参加政府采购活动。

▲《中华人民共和国政府采购法实施条例》第七十四条　有下列情形之一的，属于恶意串通，对供应商依照政府采购法第七十七条第一款的规定追究法律责任，对采购人、采购代理机构及其工作人员依照政府采购法第七十二条的规定追究法律责任：

1. 供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关情况并修改其投标文件或者响应文件；
2. 供应商按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件；
3. 供应商之间协商报价、技术方案等投标文件或者响应文件的实质性内容；
4. 属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；
5. 供应商之间事先约定由某一特定供应商中标、成交；
6. 供应商之间商定部分供应商放弃参加政府采购活动或者放弃中标、成交；
7. 供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商中标、成交或者排斥其他供应商的其他串通行为。

**第三章 评标办法及评标标准**

**第一条** 评标按下列程序进行：

（一）依法组建评标委员会；

（二）评标前准备；

（三）资格审查；

（四）技术标评审；

（五）报价评审

（六）完成评标报告。

**第二条** 采购机构依法组建由5人以上（含）奇数的人员组成的评标委员会，负责对投标文件进行审查、质询、评审和比较等。评标小组由采购单位代表和政府采购专家组成，其中政府采购专家人数不少于成员总数的三分之二。

**第三条**  评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。

**第四条** **本项目先开资信、技术文件，再开报价文件。其中资信和技术分占70%，报价分占30%。**

**第五条 本项目采用综合评分法。即在全部满足采购文件实质性要求的前提下，评标委员会对通过评审的所有投标人以总分由高到低推荐中标候选人，得分最高的投标人为排名第一的中标候选人，并进行采购结果公示。**

**资信及商务、技术评分表**

|  |  |  |
| --- | --- | --- |
| **评审内容** | **评审标准及说明** | **分值** |
| 系统整体建设方案（9分） | 对采购需求与项目背景的理解，投标人提供总体方案设计，方案包括：部署一台数据库安全审计系统、构建安全的政务网络边界、形成全局安全可视与高级威胁防护能力，方案设计合理、完整、可行，每项得3分，最高9分；方案设计存在缺陷酌情扣分，扣完为止。 | 9 |
| 投标产品响应度及符合性（25分） | 投标产品的基本功能、技术指标与需求的吻合程度和偏差情况（包括所投标产品的规格型号、详细配置、主要技术参数、随机软件、证明材料等），是否能够满足采购文件要求，带“▲”为实际业务需要，不得出现负偏离，否则做无效标处理；其他技术指标每负偏离一项，扣1分，扣完为止。注：“技术参数要求”中需要提供的资料却未提供的视为负偏离，按本项评分标准进行扣分。 | 25 |
| 功能演示（9分） | **系统现场演示：采购单位提供现场演示环境及演示账号密码，为确保演示环境安全稳定，演示前需与业主签署安全责任书。演示内容如下（未提供演示或演示不到位不得分），演示时长20分钟内。演示时间：2021年1月6日9:00，演示地址：杭州市临安区行政服务中心B座四楼1号开标室。**演示内容如下（未提供演示不得分）：1.安全感知探针：安全感知探针支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求；（以上5种日志传输模式全部演示成功的得3分，满足以上5种模式中的任意3项得1分，低于3项的不得分）。2.服务器杀毒软件：服务器杀毒软件支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到现场演示环境中的安全态势感知平台（1分）；安全态势感知平台进行分析和展示（2分）。3.日志审计系统：支持与现场演示环境中运维安全管理系统、数据库系统实施联动部署（1分）；全面实现现场演示环境中数据库业务访问、后台维护操作、网络运行日志及应用系统日志的综合审（2分）。 | 9 |
| 项目实施（6分） | 投标人组织实施方案的科学性、合理性、可操作性，提供工作时间进度表、工作程序和步骤、管理和协调方法、关键步骤的思路和要点等综合打分，最高2分。 | 2 |
| 根据项目组实施人员专业人员素质、技术能力、专业分布等情况，①项目组实施人员具有类似项目实施经历，每提供一个证明材料得1分，最高2分；②项目组实施人员资质情况，提供专业技术能力资质证书，每提供一个资质证书得1分，最高2分，同一人具有多类证书不重复计分（要求提供项目组人员近3个月的社保缴纳清单、资质证书及其他相关证明材料）。 | 4 |
| 售后维护方案（10分） | 1.指定一名运维负责人负责本项目质保维护工作；2.系统故障处理应及时予以响应（免费上门服务），响应时间为2小时，解决问题时间为48小时；3.提供3年设备产品厂商质保，质保期过后需提供终身维修服务，维修费用以原厂成本价收取。每满足一项得2分，不满足不得分，总计6分。 | 6 |
| 建立定期巡检制度、系统运行情况报告制度、用户故障响应制度，对用户故障的响应、处理、定期巡检等情况的有效性进行评价，根据相关制度制定情况，最高得2分。 | 2 |
| 培训计划包括培训内容、培训时间地点、培训对象，培训师资力量等；根据投标方案内容进行评分，最高得2分。 | 2 |
| 投标人情况（10分） | 投标人或产品厂商具备信息技术服务管理体系认证的得1分；信息安全管理体系认证的得1分（提供相关证书）。 | 2 |
| 为保证安全防护产品安全及稳定，投标人或所投安全防护产品厂商具备云安全成熟度模型CSA-CMMI 5认证的得2分；满足3-4级的得1分（提供证书复印件）。 | 2 |
| 投标人提供类似项目的成功案例，结合已完成的项目案例和用户反应情况，依照投标人提供的合同、用户验收报告。只提供合同或用户验收报告的案例，每个得1分；同时提供合同和用户验收报告的案例，每个得2分；最高得6分。 | 6 |
| 投标文件编制（1分） | 相关资料的提供情况，是否真实、完整、清晰、有序、合理；投标文件是否编制完整、格式规范、内容齐全、表述准确、条理清晰，是否与采购文件的评分要点准确设置关联点、文本图片清晰、符合招标文件要求，得2分；投标文件存在其他错漏的，每项（次）扣 0.2分；投标文件有关内容前后矛盾、与招标文件要求不一致等，评标委员会允许且需要通过询标等程序进行澄清的，该项不得分。 | 1 |

**备注：为方便专家评审，请各供应商将本表编入投标文件，并置于投标文件目录之前。**

 **第六条 评标步骤**

**1、在资格审查时，如发现下列情形之一的，投标文件将被视为无效投标：**

1）**投标人因自身原因解密失败且未提供备份文件的；**

2）投标人未能提供合格的资格文件；

3）投标人应盖公章而未盖公章、未有效授权、法定代表人授权书填写不完整或有涂改的；

4）投标文件内容虚假的；

5）投标文件的实质性内容未使用中文表述、意思表述不明确、前后矛盾或者使用计量单位不符合采购文件要求的（经评标委员会认定允许其当场更正的笔误除外）；

6）投标文件的关键内容字迹模糊、无法辨认的,或者投标文件中经修正的内容字迹模糊难以辩认或者修改处未按规定签名盖章的；

7）投标人拒绝按采购文件修正原则对投标文件进行修正的；

8）不符合法律、法规和本采购文件规定的其他实质性要求的。

**2、在商务技术评议时，如发现下列情形之一的，投标文件将被视为无效：**

1）明显不符合采购文件中规定的采购需求的响应方案；

2）与采购文件有重大偏离的响应文件；不符合采购文件中“▲”条款要求的；

3）不响应或者擅自改变采购文件实质性要求或者投标文件有采购人不能接受的附加条件的；

4）投标有效期、交货期、质保期等不能满足采购文件实质性要求的；

5）投标人技术方案不明确，存在一个或一个以上备选（替代）方案的；

6）资信及商务文件、技术文件中出现投标报价信息的。

 **▲公开招标：先公布无效投标的投标人名单、投标无效的原因及有效投标的评分结果，再开报价文件。如投标有效供应商不足三家，经评标委员会确定为废标。**

**3、报价计算**

1）全部报价中，超过项目上限价的报价无效。

2）以全部有效报价的最低价作为评标基准价，其最低报价为满分；各投标方的投标报价分统一按照[投标报价得分=（评标基准价/投标报价）\*价格权值\*100]的计算公式计算。

3）如得分相同，投标报价低者为中标供应商；如得分且投标报价相联同的，技术性能得分高者为中标供应商。

4）报价包括所选设备材料制造、运输、安装、土建、调试、税金及保修期间的维修等费用。

**4、错误修正**

报价文件如果出现计算或表达上的错误，修正错误的原则如下：

1.投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

2.大写金额和小写金额不一致的，以大写金额为准；

3.单价金额小数点或者百分比有明显错位的，以开标一览表（报价表）的总价为准，并修改单价;

4.总价金额与单价汇总金额不一致的，以单价金额计算结果为准；

5.对不同文字文本投标文件的解释发生异议的，以中文正本为准。

6.同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价按照财政部第87号令 《政府采购货物和服务招标投标管理办法》第五十一条第二款的规定经投标人确认后产生约束力，投标人不确认的，其投标无效。

**5、在报价评议时，如发现下列情形之一的，投标文件将被视为无效：**

1）以赠送方式的报价；

2）投标报价超出上限价的；

3）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

**6、不符合法律、法规和本采购文件规定的其他实质性要求的（**实质上没有响应投标文件要求的投标将被视为无效，但经评标委员会认定属于投标人疏忽、笔误所造成的差错，应当允许其在开标结束之前进行修改或者补正**）**。

**第七条 开标内容的保密**

1）开标开始后，直到宣布成交结果止，凡属于审查、澄清、评价和比较的所有资料，都不应向投标人或与开标无关的其他人泄露。

2）在投标文件的审查、澄清、评价和比较以及确定成交供应商过程中，投标人对采购机构和评审小组施加影响的任何行为，都将导致取消资格。

**第八条 投标文件的澄清**

对投标文件中含义不明、表述不一致或有明显计算错误等内容，评审小组将对投标人进行询标，并要求投标人作书面澄清；投标人的书面澄清，应由法定代表人或授权代表签字，作为投标文件的补充部分。

1. **项目技术规范、服务要求、采购需求**

**一、采购内容及技术需求**

## **（一）项目名称**

杭州市临安区机房信息数据安全保护设备采购建设项目。

## **（二）项目性质**

本项目为新建类项目。

### **（三）项目建设思路**

临安区电子政务外网网络安全防护建设主要建设思路是：在保证业务稳定、高性能的基础上，全面提高网络边界的整体安全防护能力，重点加强项目方案可实施性，易运维管理性，提升方案实施和日常运维效率。相关思路如下：

（1）部署一台数据库安全审计系统。既能独立审计针对数据库的各种访问行为，又不影响数据库的高效稳定运行。

（2）构建安全的政务网络边界。通过统一互联网出口处的外界隔离防护、入侵检测，减少威胁的攻击面以及漏洞暴露时间；通过划分网络安全域，加强安全域边界的防护，隔离受感染的区域，降低入侵威胁造成的损失；通过终端的网络准入机制进行策略遵从和强制策略执行，实施网络接入与终端安全管理，等等。

（3）形成全局安全可视与高级威胁防护能力。在网络边界防护、内网威胁检测与识别的基础上，需要进一步形成全局的安全可视能力。同时实现高级威胁防护，如APT攻击、勒索病毒、0Day漏洞攻击等安全防护能力。

### **（四）项目建设目标**

对临安区政务网络安全进行规划建设，保障业务的安全与稳定运行，同时同步规划建设网络安全技术和管理体系，根据等级保护2.0标准完善网络安全等级保护建设。进一步完善临安区政府网络安全管理支撑体系和安全技术保障体系。主要包括基于全区安全平台一期基础上，建设临安区全网安全运营中心，实现对全网安全的预警分析，同时对临安区数据平台云主机进行联动管理，最终构造覆盖网络和数据中心全网安全运营管理体系，提升网络安全防护及管理能力。最终完善系统网络安全防护技术措施，提升系统技术防护能力，满足第三级系统网络安全等级保护相关技术要求。

本次项目其他要求：第一，能对于临安当下的网络资源和安全设备合理利用，能纳管联动的统一联动；第二，能够满足未来3-5年的信息化政务发展需求。

1. **项目建设内容**

政务外网-网络安全建设：

政务外网出口：建设安全防护措施，入侵防御1台，上网行为管理系统1台,服务器杀毒软件200套。

政务外网运维区：日志审计系统1套，数据库审计系统1套，安全态势感知系统1套，运维安全能管理系统1套。

### **（六）项目建设周期**

本项目建设总工期估算约4个月，项目建设1个月，试运行3个月。

**（七）项目采购清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类别 | 序号 | 产品名称 | 配置说明 | 数量 |
| 网络安全系统 | 1 | IPS | 性能参数：网络层吞吐量：50Gbps，并发连接数：4100000，新建连接数：300000。硬件参数：规格：2U，内存大小：16G，硬盘容量：64GB MSATA SSD+1TB SATA，电源：冗余电源，接口：6千兆电口+4个光口+4万兆光口SFP+。 | 1 |
| 2 | 上网行为管理系统 | 性能指标：网络吞吐量10Gb、推荐带宽5Gb、支持用户数50000、每秒新建数80000、最大并发数3200000；硬件指标：2U，双电源，4个千兆电口，4个千兆光口，2个万兆光口，1个串口(RJ45) ，2个USB2.0，24G内存，SATA硬盘1TB+64G SSD; | 1 |
| 3 | 日志审计系统 | 2U，处理性能10000条/秒，RAID、热插拔硬盘、可用存储量8TB，4个千兆电口，16GB内存，支持3路千兆监听；支持Windows、Linux等操作系统、支持网络设备（交换机、路由器、UTM等）、安全设备（防火墙、VPN、IPS、IDS、防毒墙、安全网关等）、数据库系统、网络行为、中间件（Tomcat、Webspere、weblogic等）应用系统（Web服务器、邮件服务器、OA、CRM等）日志集中管理与审计；不限审计授权许可数量；无限日志源； | 1 |
| 4 | 数据库审计系统 | 2U，处理性能10000条/秒，RAID、热插拔硬盘、可用存储量8TB，4个千兆电口，16GB内存，支持3路千兆监听；支持Oracle、MSSQL、Mysql、Sybase、DB2、Informix六大类关系型数据库和达梦、南大通用、人大金仓等国产数据库操作行为审计；支持15个以上数据库类型，无限个数据库许可。 | 1 |
| 5 | 安全感知探针 | 性能指标：1.5Gbps，硬件指标：2U，SATA 1T、单电源，标配4个千兆电口+4个千兆光口； 潜伏威胁探针主要通过旁路部署方式对全流量信息进行采集； | 1 |
| 6 | 运维安全管理系统 | 2U，支持所有主流图形终端、字符终端、文件传输和数据库管理，支持HTTP/HTTPS、KVM和第三方软件（如Radmin、Pcanywhere），RAID，热插拔硬盘、可用存储容量4TB，4个千兆电口，16GB内存，可扩展8个千兆电口或光口，内置600个主机/设备操作监控许可证，最大2000个并发会话连接数 | 1 |
|  | 7 | 服务器杀毒软件 | 包含Webshell检测、暴力破解检测、僵尸网络检测、基线合规检查，杀毒等 | 200 |
|  | 9 | 维保 | 三年 |  |

## **（八）招标参数**

## 1.入侵防御IPS

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 性能配置 | 性能参数：网络层吞吐量：50Gbps，并发连接数：4100000，新建连接数：300000。硬件参数：规格：2U，内存大小：16G，硬盘容量：64GB MSATA SSD+1TB SATA，电源：冗余电源，接口：6千兆电口+4个光口+4万兆光口SFP+。 |
| 部署方式 | 支持路由模式、透明网桥部署、旁路部署、单臂部署以及混合部署等多种方式； |
| 网络特性 | 支持802.1Q VLAN Trunk、access接口类型，VLAN三层接口和子接口； 支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路； |
| 路由支持 | 支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能（投标时需提供截图证明文件）； |
| 应用识别与流量控制 | 支持P2P、IM、游戏、炒股软件、网银，流媒体，常用邮件以及远程控制软件等的识别和控制，支持识别管控的应用类型超过1200种，应用识别规则总数超过3000条； |
| URL过滤 | 内置海量URL分类库，包含非法及不良网站、成人内容、网上购物、微博论坛等分类，实现全面高效的不良网站过滤。 |
| 内容安全防护 | 支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于AI技术的病毒检测报告（投标时需提供相关功能截图证明）； |
| 入侵检测功能 | 设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上（需提供截图证明） ；支持间谍软件、后门、蠕虫等恶意软件防护；支持同访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间； 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（投标时需提供截图证明文件）； |
| 僵尸主机检测 | 设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在60万条以上； 支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机IP地址；（投标时需提供截图证明文件）； |
| 安全可视化 | 支持全网实时热点事件TOP10展示；支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持基于攻击阶段图的方式来匹配并展示当前用户遭受到攻击的具体所处状态，并详细给出针对性处理建议，便于用户快速响应安全问题（需提供产品功能界面截图证明）；  |
| 用户认证 | 支持本地密码认证，LDAP、Radius等服务器外部密码认证方式，支持基于域、Proxy、Pop3、Web、Radius单点登录方式； |
| 安全集中管理 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志实时上报与展示等功能； |
| 系统管理 | 支持安全策略一体化配置，通过一条策略快速实现不同安全功能的配置，简化策略配置工作； 支持本地设备安全日志上传云端安全平台分析确认，可识别持续性攻击、黑链、高危僵尸病毒等高级威胁并通过微信方式进行预警；支持高级威胁关联分析的能力，并展示热点事件详情，推送到运维管理员手机中进行快速处置（投标时提供相关功能截图证明）；支持设备软硬件异常状态监控，可以监控设备CPU、内存、硬盘使用率，并且可监控系统状态、网络接口状态、安全能力监控状态，帮助用户实时了解安全设备运行状况；  |
| 日志管理 | 支持SYSLOG标准日志协议；安全日志根据日志类型可存储在产品内置数据中心、外置数据中心、Syslog日志服务器、安全感知系统多种方式； |
| 云端联动 | 支持与安全云实现联动，当本地无法判断恶意样本、恶意域名、恶意URL时，可以实时上传到安全云脑，通过云端沙箱、威胁情报、云端黑白名单机制实现对威胁的实时阻断，针对恶意文件给出文件鉴定报告（投标时需提供产品功能截图证明）。  |

## 2.安全感知探针

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 性能配置 | 吞吐性能：1.5Gbps。硬件参数：内存大小：8G，硬盘容量：1T SATA，电源：单电源，接口：4千兆电口+4千兆光口SFP。 |
| 部署模式 | 旁路部署，支持接入多个镜像口，每个接口相互独立且不影响。 |
| 安全体系化能力 | ▲本次投标的安全感知探针为我单位已使用且成熟稳定的安全态势感知平台的基础上进行加点建设，为保障安全的连续性，本次建设基于现有的安全感知平台基础进行建设。 |
| ▲支持与安全感知平台（进行数据对接、防御联动及策略关联，对本系统检测数据进行统一展现，并对检测的数据以风险类型、威胁等级在安全感知平台实现自动化编排响应处置手段，将自定义的安全事件处置策略转化为自动响应策略，解决同类型手动重复配置问题，减轻运维压力（中标后7个工作日内需提供厂商承诺函盖章原件）； |
| ▲本系统支持将检测的数据及安全风险对接上传到安全感知平台，并能识别现有平台已对接的安全设备，自动推荐联动策略：包括联动现有防火墙封锁、访问控制；联动本次采购的上网行为管理进行上网提醒、冻结账号；联动杀毒软件进行一键查杀、进程取证（中标后7个工作日内需提供厂商承诺函盖章原件）。 |
| 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 |
| 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意UR监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录。 |
| 网站攻击检测 | 支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等网站攻击检测（需提供截图证明）。 |
| 敏感信息检测 | 支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤（投标时需提供截图证明）； |
| 日志传输 | 安全感知探针支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求； |
| 漏洞利用攻击检测 | 支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Network Device、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测（投标时需提供截图证明）。 |
| 支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测 |
| 支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、VNC等协议暴力破解检测。 |
| 异常流量检测 | 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等（需提供产品截图证明）。 |
| 支持ICMP、UDP、SYN、DNS等协议外发异常流量检测，支持自定义阀值。 |
| 特征库 | 产品内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。 |
| 僵尸网络行为检测 | 支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。 |
|  | 支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志 |
| 支持传输访问检测日志，包括正常访问、风险访问、违规访问 |
| 支持传输协议审计日志，包括https协议日志、http协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、AD域协议审计日志、WEB登录审计日志、FTP协议审计日志、Telnet协议审计日志、ICMP协议审计日志、LLMNR协议审计日志； |
| 违规访问检测 | 支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式（需提供截图证明）。 |
| 沙盒对接 | 支持将流量还原的文件发送至沙盒分析；可支持第三方沙盒对接。 |
| 特征库 | 内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库 |
| 抓包分析 | 支持流量抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式（投标时需提供截图证明文件）； |
| 管理功能 | 支持设备内置简单命令行管理窗口，便于基础运维调试；可实时监控设备的CPU、内存、存储空间使用情况；能够监控监听接口的实时流量情况。 |

## 3.服务器杀毒软件

|  |  |
| --- | --- |
| 产品形态 | 产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署；单一管理控制中心可统一管理分别部署在Windows PC，Win服务器以及Linux服务器的客户端软件 ； |
| 授权 | 提供200点pc/服务器终端授权； |
| 全网威胁展示 | 支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量； |
| 支持展示全球热点风险事件在网内终端的爆发情况，及时了解、处置网内终端的热点风险事件，并显示影响终端数量； |
| 微隔离之流量可视 | 支持基于IP（组）、服务和角色维度进行配置项设置，并且支持对配置项的备份以及恢复操作； |
| 业务系统详情支持展示流量分布Top5、业务流量排行Top5(发送，接收)、业务访问趋势（发送流速、接收流速和用户数）； |
| 流量线详情支持展示该流量线对应的控制策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等； |
| 脚本批量下发 | 支持管理平台向终端下发脚本（.bat，.sh和.ps1）执行文件，方便管理人员对终端进行脚本下发； |
| 补丁管理 | 支持对终端的漏洞情况进行扫描，并查看漏洞具体情况及KB号，并显示具体修复情况 ； |
| 支持流行Windows高危漏洞的轻补丁免疫防御，支持支持Windows补丁批量一键修复； |
| 终端配置管理 | 支持收集并展示单个终端的基本信息，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端agent版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新； |
| 支持对系统高危端口执行一键封堵； |
| 资产梳理 | 支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑root权限账号、长期未使用账号、夜间登录、多IP登录进行账号分类查看，支持统计最近一年未修改密码的账户支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示（投标时需提供截图证明）； |
| 威胁检测 | 备基于本地缓存信誉检测与全网信誉检测，构建全网信誉库的检测引擎，做到内网一台威胁，全网感知并进行针对性查杀，支持处置病毒时选择是否在其它终端上同步处置有效提升查杀效率，减少终端资源开销； |
| 支持本地查杀缓存，具备二级缓存机制：终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗； |
| 支持基于威胁情报的病毒特征值和域名全网终端搜索，可定位出全网终端该病毒的感染情况（需提供产品截图证明）； |
| 文件实时监控 | 可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好设置高、中、低3种防护级别； |
| 勒索病毒专防 | 基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御（投标时需提供产品截图证明）； |
| 支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截； |
| 支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具； |
| 挖矿病毒巡检 | 提供挖矿病毒巡检工具，支持通过内存、进程和启动项来检索病毒相关信息； |
| 终端合规检查 | 支持对Windows、Linux终端提供一键式操作对指定终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示终端的基线合规检查结果 |
| 统计报表 | 支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议（需提供产品截图证明）； |

## 4.上网行为管理(核心产品）

|  |  |
| --- | --- |
| 指标项 | 主要技术参数 |
| 性能配置 | 性能指标：网络吞吐量10Gb、推荐带宽5Gb、支持用户数50000、每秒新建数80000、最大并发数3200000；硬件指标：2U，双电源，4个千兆电口，4个千兆光口，2个万兆光口， 1个串口(RJ45) ，2个USB2.0，24G内存，SATA硬盘1TB+64G SSD; |
| 部署方式 | 要求设备支持网关模式，支持NAT、路由转发、DHCP等功能；支持网桥模式，以透明方式串接在网络中；支持旁路模式，无需更改网络配置，实现上网行为审计；支持两台及两台以上设备同时做主机的部署模式； |
| 终端管理 | 自动发现网络里面的终端，并获取IP、Mac、厂商、操作系统、开放服务、开放端口等信息，支持根据ip段、MAC、使用者过滤用户，以便和其他过滤方式一起组合来搜索或获取终端信息； |
| 离线管理，在非内网环境下实现客户端应用审计、U盘审计、IM审计，外发行为日志留存在终端本地，已配置的外设管控、外联管控、访问控制策略保持生效，终端接入内网后同步到设备日志中心。 |
| 设备必须支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，支持移动终端型号识别，至少识别不少于10种移动终端型号；（提供产品界面截图） |
| 安全体系 | 支持与本次投标的态势感知平台进行联动响应，同步关联安全事件，支持在态势感知平台上一键联动上网行为管理，推送用户提醒与冻结用户上网（投标时提供截图证明文件）； |
| IPv6支持 | 支持部署在IPv6环境中，相应的所有功能（上网认证、应用控制、内容审计、报表等等）均都支持IPv6（投标时需提供产品截图证明）； |
| 链路负载 | 为了提高出口多链路利用率，要求支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载。支持使用VPN做专线备份，支持链路故障检测（投标时提供截图证明文件）； |
| 杀软检查 | 支持20款以上主流杀毒软件的运行情况、软件版本、病毒库更新时间检查，对不满足检查要求的终端可重定向页面修复、弹窗提示、限制权限、禁止上网；（投标时需提供截图证明文件）； |
| 自定义任务 | 支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网（投标时需提供截图证明文件）； |
| 外联检查 | 支持自动检查终端是否能PING通互联网地址，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户； |
| 支持检查终端是否使用双网卡，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户； |
| 业务需要 | 为减少短信费用投入，要求设备支持微信身份验证，用户可以通过微信“扫一扫”、关注公众号等操作获取上网权限，后台能够记录下用户微信的ID，支持与第三方微信平台对接，无需修改第三方平台代码； |
| IP管理：支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量（投标时提供产品功能截图）；终端资产业务可视管理：1. 对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等；

2）支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3）支持查看终端类型分布。  |
| 支持非法外联行为检查阻断，包括拨号、双网卡、有4G网卡、有无线网卡、连接非法wifi、使用非法网关、私连外网、自定义外联等行为，对不满足检查要求的终端强制断网，向管理员告警，并弹窗提示用户（投标时需提供产品截图证明）； |
| 针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测（提供功能截图证明）； |
| 为满足访客PC的简易接入授权，访客终端接入无线网络后，终端自动弹出二维码页面，审核人通过手机扫描访客终端二维码，添加备注信息，访客即可完成上网，同时设备记录访客备注信息、接入终端MAC以及审核人帐号； |
| 为确保我单位不会通过SSL加密内容发生通过互联网出口泄密事件，要求设备必须能够识别并过滤SSL加密的钓鱼网站、金融购物网站；识别和审计加密的邮箱（如GMAIL）等； |
| 应用识别规则库 | 支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类；此外可根据我单位需求自定义标签，根据标签做应用控制； |
| 应用控制 | 设备内置应用识别规则库，支持超过6700条应用规则数，支持超过2900种以上的应用，1000种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； |
| 流控黑名单 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（投标时需提供产品截图证明）； |
| P2P智能流控 | 要求设备有效抑制如迅雷、ppstream等P2P应用带宽，通过抑制可看到出口上下行带宽的明显改善（投标时需提供产品截图证明）； |
| IM审计 | 支持对QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计 |
| SSL加密内容审计和过滤 | 支持识别并过滤SSL加密的钓鱼网站、金融购物网站、非法网站等，同时支持SSL硬件加速卡解密，从而可提高SSL全流量解密性能； |
| 上网安全 | 设备必须内置业界知名杀毒引擎，支持防ARP欺骗，支持告警；支持定时广播静态ARP表项； |
| 支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为（包括包括钓鱼及恶意网站、漏洞利用、挖矿页面、恶意跳转、跨站脚本攻击和病毒文件等），避免用户网页资源被滥用；支持实时阻断和告警； |
| 具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证；支持识别、阻断、冻结（指定时长）僵尸主机，并推送同品牌端点安全软件进行查杀； |
| 外发管理 | 支持HTTP上传/FTP/邮件附件等形式的外发文件行为，支持基于扩展名识别并拦截外发文件； |
| 单用户行为分析 | 针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等） |
| 数据分析应用 | 数据中心可以对上网日志进行大数据分析，并支持多个大数据分析模型，包括泄密分析、离职倾向分析、上网态势分析、带宽分析、工作效率分析，可导出报表； |

## 5.日志审计系统

|  |  |
| --- | --- |
| 指标项 | 主要技术参数 |
| 产品资质 | 产品必须是自主研发而不是OEM产品； |
| 产品结构 | 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； |
| 产品架构 | 采用标准2U机架式硬件；RAID，热插拔硬盘；16GB内存 |
| 操作系统 | 深度定制优化的Linux系统； |
| 管理方式 | B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 设备部署 | 提供旁路接入模式，设备部署不影响原有网络结构； |
| 数据存储 | 所供系统设备必须自带本地存储功能；禁止采用通用关系型数据库来存储日志；物理磁盘空间2\*8TB；日志存储量至少八十亿条；RAID架构以保证数据可靠性,支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)； |
| 网络接口 | 审计主机至少提供千兆RJ45\*4（一路数据传输口；一路系统管理口）；网络接口支持电口，可升级为光口； |
| 处理性能 | 日志采集能力：10000条/秒以上 |
| 数据采集 | 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]；支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]支持Opsec Lea日志采集；支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控（投标时提供截图证明文件）；支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储；支持文本型日志原始文件管理，可将系统作为日志服务器使用；支持FTP行为审计并提供FTP二次登陆系统及实现文件传输和过程监控的方法技术（投标时提供证明文件）；支持Telnet行为审计并提供一种安全终端仿真协议监控时实现会话复制和跟踪的方法技术（投标时提供证明文件）； |
| 监控功能 | 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况；支持自定义配置实时监控的日志类型；支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警；支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况；支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作； |
| 报表分析功能 | 系统内置多种类报表模板；支持动态\静态（日报、周报、月报）两种系统生成方式；支持报告的邮件转发、生成提醒功能；支持多人邮件接收；支持自定义审计报告；支持导出html、Excel、PDF；支持管理员自定义审计报表模板； |
| 查询分析功能 | 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索；支持以日志类型、时间范围及条件字段快速检索过滤；支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询；支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件；支持查询模版创建、修改、删除功能；支持查询结果导出； |
| 策略管理功能 | 支持内置归并策略，对HTTP数据进行自动归并处理；支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件；支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问；支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略； 规则条件设定支持逻辑运算符与支持正则表达式；支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息；支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息； |
| 数据管理功能 | 支持按日志属性、日志类型、时间范围进行数据备份；支持WEB界面备份及日志恢复导入工作；支持自动与手动两种备份归档方式；系统支持以FTP上传方式将归档文件存储到第三方存储系统中； |
| 系统配置功能 | 支持审计系统用户（组）管理（添加、修改、删除、停用、启用）；支持资产管理，即所有采集日志源管理维护；支持密码长度、复杂度，密码猜测自动锁定账号以及系统超时设置安全策略；支持证书页面生成下载；支持系统配置备份恢复；支持时间同步页面配置；支持页面方式系统升级以及设备关闭、重启；支持从WEB界面查看网卡IP设置，修改静态路由设置等内容；支持安全页面（SSL）证书下载； |
| 系统自身安全 | 系统内置安全防火墙；支持控制访问审计主机范围；必需提供内部通讯检查机制，传输128加密；管理接口支持串口或电口的方式管理；管理界面与其他功能模块分离； |
| 日志数据安全 | 审计日志文件方式存储；审计日志加密导出审计系统；支持对所有审计管理员操作审计系统的动作进行审计； |
| 日志权限 | 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明；支持日志类型、IP地址权限设置；支持页面功能模块权限设置； |
| 系统升级二次开发 | 在设备维保期内，厂家提供对系统软件的免费升级服务，保证系统软件为最新版本；根据用户需求定制开发相关内容，包括关联报表和特定业务日志审计等功能； |
| 系统许可方式 | 永久许可方式，再增加审计用户的情况下不用增加授权许可；无限日志源（投标时提供截图证明文件）。 |

## 6.数据库审计系统

|  |  |
| --- | --- |
| 指标项 | 主要技术参数 |
| 产品结构 | 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； |
| 产品架构 | 采用标准1U机架式硬件；热插拔硬盘，16GB内存 |
| 操作系统 | 深度定制优化的Linux系统； |
| 管理方式 | B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| 设备部署 | 提供旁路接入模式，设备部署不影响原有网络结构； |
| 数据存储 | 1. 所供系统设备必须自带本地存储功能；
2. 禁止采用通用关系型数据库来存储日志；
3. 物理磁盘空间8TB；日志存储量至少八十亿条（指标以原厂公开资料为准）；
4. RAID架构以保证数据可靠性（指标以原厂公开资料为准）；
5. 支持后期扩展外部网络存储(IP SAN、NAS、DAS、磁盘阵列等)；
 |
| 网络接口 | 1. 审计主机至少提供千兆RJ45\*4（一路数据传输口；一路系统管理口）；
2. 网络接口支持电口，可升级为光口；
 |
| 日志生命周期管理 | 包括日志采集、实时分析、存储备份、审计报告功能； |
| 处理性能 | 日志采集能力：10000条/秒以上 |
| 审计对象范围 | 全面支持DB2、Oracle、MSSQL，MYSQL、Informix、SyBase、达梦、人大金仓、南大通用、神通、Postgresql、cache、Mongo、Teradata，、以及Telnet 、FTP、SSH、RDP、VNC（投标时提供截图证明文件）； |
| 必备功能 | 1. 审计系统支持以syslog、snmp trap、opsec lea、WMI等标准协议接口采集各类日志数据；
2. 审计系统自动将采集的操作语句解析为查询、增改、删除、过程等类型呈现；
3. 审计记录包括行为发生时间、员工工号、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、返回结果等关键信息。
4. 提供工号信息接口，将数据库操作语句与操作者工号建立关联关系，实现操作者实名认证；
5. 审计系统能够对未经许可的客户端工具直接访问数据库的行为实施阻断；
6. 支持配置操作行为解析模型（黑白名单），灵活区别正常操作和异常操作事件；
7. 支持依据语句解析模型，以操作频率为条件实施行为阻断；
8. 支持将可疑的数据库查询语句以在线的方式反显执行，并即时在线查看返回结果；
9. 支持将异常操作的完整会话信息进行前后操作语句关联查看分析；
10. 支持分中心部署方式，能够配置分支数据集中上传至中心机；
11. 扩展性强，能够与运维安全审计、日志综合审计、应用系统审计整合成统一安全审计平台；
 |
| 实时分析功能 | 1. 提供力导向图，可实时查看当前数据库的连接情况，并通过对节点的点击展示更加详细的信息；
2. 支持网络审计，可定期获知数据库服务器是否存在非数据库的访问通讯，以协助判断潜在风险；
3. 实时窗口以多种图形方式展示流量分析、事件分析、告警分析及综合分析结果；
4. 流量分析：以业务系统工号为基线，统计分析当天某段时间（自定义）内的操作流量；
5. 事件分析：依据安全策略，以时间为基线，统计异常事件的发生数量和趋势；
6. 告警分析：依据安全策略，以时间为基线，统计严重告警事件的发生数量和趋势；
7. 综合分析：以数据库操作类型为基线统计各类操作状况，并统计审计系统资源以及系统操作的状况；
8. 实时操作数据以不同等级（丢弃、过滤、安全、重要、事件、告警）进行分类显示；
9. 支持因子监测功能，对数据库中突发增加的内容提供独立展示页面。因子内容包括：IP地址、应用程序名、计算机名、存储过程、数据库用户名、数据名、数据库主机。系统记录因子出现次数，且能排序，可多维快速定位因子（投标时提供截图证明文件）；
10. 实时操作语句直接以查询、增改、删除、过程等操作类型分类显示；
11. 支持SQL模板，系统能自动识别并抽取数据库句式语意相同但参数不同的语句，并通过独立页面展示，同时记录该模板的状态、触发规则名、总记录数、总告警数、上次告警记录数、上次出现时间、最后出现时间，并能设置该模板别名（投标时提供截图证明文件）；
 |
| 审计分析报告 | 1. 系统默认报告数量不少于百种；
2. 以图(柱、曲线、饼等)，统计、明细数据的方式表现；
3. 支持动态\静态（日报、周报、月报）两种系统生成方式；
4. 支持报告模版创建、修改、删除功能；
5. 支持报告的邮件转发、生成提醒功能；支持多人邮件接收；
6. 支持自定义审计报告；
7. 支持多层嵌套报告；
8. 支持报告自定义归类；
9. 支持导出html、Excel、PDF；
10. 报告名称以树型菜单统一高效管理；
 |
| 查询检索 | 1. 日志数据全字段检索至少满足500万条<5秒；
2. 支持多条件组合查询方式；
3. 支持逻辑运算符(或、与、非)；
4. 支持正则表达式；
5. 支持IP、字符、数字、日期、时间等日志字段；
6. 支持查询模版创建、修改、删除功能；
7. 支持历史查询任务列表的查看；
8. 支持查询结果导出；
9. 支持日志字段自定义选择显示；
 |
| 分析策略 | 1. 全局策略：支持以服务器IP、数据库类型、数据库表、操作类型（查询、增改、删除等）设定策略，采集（过滤）核心关注（无关紧要）的数据，将操作数据进行分类（安全、重要、事件、告警等）入库；
2. 模型分析策略：支持以入库的操作语句为原型，根据获取的语句内容片段、数据库表名、条件字段、操作频率以及结果影响行数设定分析策略（黑白名单），区分正常操作和异常告警操作；
3. 三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息；实时规则策略：支持根据日志字段为条件预设置分析策略；
4. 系统内置策略模板，可以直接加载生效；
5. 支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息；
 |
| 备份归档 | 1. 支持以日志属性、日志类型、存储周期的方式选择备份；（提供产品页面截图证明）
2. 支持归档日志恢复导入；
3. 支持自动与手动两种归档策略；
4. 支持本地、FTP上传等归档方式；
 |
| 系统管理 | 1. 支持审计系统帐号、组管理（添加、修改、删除）；
2. 支持资产管理，即所有采集日志源管理维护；
3. 支持页面升级；
4. 支持页面重启、关机；
5. 支持时间同步设置；
6. 支持系统配置导入、导出；
 |
| 系统安全 | 1. 系统内置安全防火墙；支持控制访问审计主机范围；
2. 必需提供内部通讯检查机制，传输128加密；
3. 管理接口支持串口或电口的方式管理；
4. 管理界面与其他功能模块分离；
5. 产品拥有强大的数据库入侵检测规则库，能够对数十种针对数据库的常见漏洞和攻击手法进行检测，比如SQL注入，存储过程攻击，版本检测攻击，缓冲区溢出攻击，目录遍历攻击，拒绝服务攻击，权限绕过攻击，文件异常攻击等（投标时提供截图证明文件）；
 |
| 日志数据安全 | 1. 审计日志数据以文件方式存储；
2. 审计日志加密导出审计系统；
3. 支持所有审计管理员操作审计系统的动作进行审计；
4. 支持记录审计系统之间的物理、逻辑状态变化；
 |
| 日志权限 | 1. 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明；
2. 支持日志类型权限设置；
3. 支持IP地址权限设置；
4. 支持页面功能模块权限设置；
 |

## 7.运维安全管理系统

|  |  |
| --- | --- |
| 指标项 | 主要技术参数 |
| **产品资质** | 产品必须是自主研发而不是OEM产品； |
| **产品架构** | 软硬件一体化产品，采用标准机2U架式硬件结构；热插拔硬盘； |
| **部署方式** | 旁路代理模式，不影响正常业务流量；支持HA双机部署； |
| **管理结构** | B/S架构，采用HTTPS方式远程安全管理，无需安装管理客户端； |
| **网络接口** | >=100/1000M RJ45\*4个自适应以太网口；可扩展8个千兆电口或光口 |
| **数据存储** | 设备内置存储系统，存储空间不低于4TB，采用RAID磁盘阵列；16GB内存 |
| **可管理对象数量** | 内置600个主机/设备操作监控许可证书； |
| **并发会话数** | 图形并发会话数>=500字符型并发会话数>=2000 |
| **支持协议** | 字符型远程操作协议：SSH(V1、V2)、TELNET、RLOGIN、AS400；图形化远程操作协议：RDP、VNC、X11；文件传输协议：FTP、SFTP； 数据库远程操作协议：支持ORACLE、MSSQL、Sybase、Mysql、DB2数据库远程访问协议审计；支持通过应用发布的代理进行协议扩展，支持Radmin、Pcanywhere、 HTTP/HTTPS，可定制开发其它访问协议及客户端支持；应用发布代理支持RemoteAPP穿透方式；支持协议端口自定义； |
| **服务器访问方式** | Web访问方式:通过系统的Web页面控件直接访问服务器或通过WEB页面调用本地工具（含数据库官方客户端）直接访问服务器；多种类浏览器支持：IE（6-9）、firefox、chrome、safari；web方式访问支持所有远程协议；web访问方式支持历史访问配置参数自动记忆功能；web访问方式支持直接输入目标IP快速连接功能；通过web方式使用SSH协议支持clone session功能；支持直接调用SFTP功能；支持设定窗口颜色、保存屏幕内容、打印屏幕内容、复制粘贴等功能（提供相关Web页面截图证明）；通过web方式使用图形化远程操作协议，支持自适应浏览器窗口大小；通过web方式使用RDP协议支持剪切板、磁盘映射功能； |
|  | 客户端访问方式：支持通过管理员常用的客户端(如SecureCRT、PUTTY、Mstsc、PLsql、SQLplus等)直接连接堡垒机再访问到服务器；支持客户端(SecureCRT、putty)clone session功能；支持secure shell client软件中直接调用sftp功能； |
|  | 登录资源菜单访问：客户端访问审计系统即可显示用户能访问的主机资源菜单，用户通过字符菜单或图形菜单选择列表方式直接访问服务器；菜单方式访问支持所有协议；  |
| **身份认证及访问授权** | 支持多种认证方式：本地密码认证、UsbKey认证、第三方CA证书认证、RSA动态口令认证、安盟动态口令认证、RADIUS认证、LDAP认证、AD域认证以及短信认证（提供截图证明文件）**;**支持系统自带的Usbkey和Token令牌强身份认证模式； 内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色；支持SSO功能，运维人员不必输入服务器帐号及密码，无需进行二次登录认证；支持基于用户（用户组）、目标设备（设备组）、系统帐号、协议类型、生效时间范围、源IP地址等条件组合设置访问控制策略；支持粗放式访问授权模式，授权条件仅基于运维用户（用户组）和目标主机IP地址段，不限制使用的系统账号及协议等其它条件；支持审批模式：运维用户访问特定的服务器设备必须经过管理员的临时审批授权才能进行，否则无法进行任何操作；支持备注模式：运维用户访问服务器前必须先填写该次访问的维护目的等内容，否则不能进行访问操作；支持工单授权功能：通过运维人员申请或管理员下发工单的方式来赋予运维人员访问目标服务器的权限，且有工单生效时间限制；支持登录预处理命令设置；支持设定会话连接单位时间内空闲无操作，连接自动断开；支持运维用户多次登录失败自动锁定账号功能及解锁机制设定； |
| **访问控制及异常告警** | 支持按用户（用户组）、目标设备（设备组）、系统帐号、命令集和生效时间等内容或按访问授权策略设定安全事件规则；支持指令黑白名单； 支持对违规操作的指令（黑名单）进行告警、忽略处理、自动阻断或指令审批；支持以屏幕、邮件、SYSLOG、Snmp Trap、短信方式实时发送告警信息； |
| **用户管理功能** | 支持添加、删除、修改以及启用、停用运维用户；支持用户账号批量导入导出功能；支持运维账号使用有效期管理；支持运维用户密码强度管理；支持用户组管理，可方便添加、删除、修改组信息及组成员； |
| **主机管理功能** | 支持添加、删除、修改主机内容；支持主机组管理功能，可方便添加、删除、修改组信息及组成员；支持系统类型管理：内置常见系统类型，可自定义添加目标设备的系统类型及内容，包括显示图标、该系统拥有的协议及默认端口等内容；支持在线ping主机功能，即时获取该主机存活信息；支持主机账号及协议通道验证功能，即时获知该账号及访问通道是否有效；支持主机登录限制，同一台服务器可以只允许一个用户登录，防止已登录用户被登出；支持IP地址集、时间集、指令集管理功能； |
| **操作行为记录** | 针对SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；针对RDP、VNC、X11等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息；能够记录RDP协议中的活动窗口名称、删除文件等动作，并能记录RDP会话中的键盘输入信息； |
| **会话过程回放** | 支持以WEB在线视频回放方式重现维护人员对服务器的所有操作过程，无须在客户端安装播放客户端软件；支持倍速/低速播放、拖动、暂停、停止、重新播放等播放控制操作；支持从特定操作指令开始进行定位回放；支持回放界面中显示键盘输入、功能键、鼠标动作；支持下载回放文件到本地保存，并通过厂家专用播放器查看，防止会话视频记录泄密； |
| **密码管理** | 支持按设备（设备组）、系统帐号、计划执行时间、改密周期、密码策略、改密结果发送等生成详细的改密计划，到期自动执行；支持随机生成不同密码、随机生成相同密码以及手工指定相同密码的密码策略，并能严格遵守密码强度设置；支持手工改密功能；支持改密结果自动发送至密码管理员或FTP上传；支持手工下载全部或部分主机密码功能；支持自动改密结果报表； |
| **实时监控** | 支持实时监控近期发生的所有会话信息，显示会话状态（连接中、退出、阻断）；支持对会话进行同步监控，执行会话回放、监控和阻断操作；支持Vi、Smit、rhel下setup等图形或菜单操作进行全程同步监控；支持实时监控审计系统CPU、内存、磁盘的使用情况；支持记录审计系统自身的管理操作，保障审计系统自身安全； |
| **历史查询及审计报表** | 支持单一条件快速查询、查询结果二次过滤以及多重条件组合高级查询功能；支持同一次会话中的指令关联查询，显示会话中所有操作指令；支持根据查询结果直接定位视频文件，回放历史会话；系统内置多种运行维护报表模板；支持以html、CSV或PDF方式生成并导出报表；支持管理员自定义审计报表模板；支持以日报、周报、月报的方式自动生成周期性报表，并自动发送至指定邮箱； |
| **数据安全管理** | 支持自动归档和手动备份、支持以FTP/SFTP等方式自动上传归档数据；支持备份数据恢复导入；支持空间自管理功能，存储空间不足时能够自动清理老的数据；支持系统配置的导入、导出功能； |
| **协同操作** | 支持双人协同操作功能； |
| **批量执行** | 支持批量执行功能；支持会话批量连接登录功能；支持对批量执行结果进行成功或失败判断；  |
| **消息中心功能** | 支持工作任务流程及消息中心管理功能：支持用户间互相发送消息，通过消息下发工作任务等功能；支持关键事件自动生成消息如：二次审批、备注审批、协同操作邀请；支持专用消息接收客户端（投标时提供截图证明文件）； |
| **系统管理功能** | 支持页面证书下载；支持页面下载系统相关软件；支持时间同步功能；支持从WEB界面修改网卡IP设置、静态路由设置等内容；支持修改不同访问模式（客户端直连、菜单方式）的默认访问端口；支持从WEB管理界面重启、关闭设备；支持页面超时设置；支持通过web界面进行系统升级；支持系统告警日志发送； |

1.上述采购需求中的原厂质保服务要求须在中标后提供三年原厂质保承诺原件，否则取消中标资格。

2.投标人可参考采购单位推荐的参数配置，标注▲为实际业务需要，不得出现负偏离，否则做无效标处理。同时所投标产品功能需满足本单位要求，中标后7个工作日内提供样机测试，若产品功能不能满足或不能按时提供样机，取消中标资格。

1. **项目验收标准**

验收主要以采购文件定义的软、硬件技术参数要求为标准，严格按照各项参数要求对相应的硬件、软件及整体平台架构进行验收。中标单位制定具体的供货计划，并在到货前至少5个工作日通知采购人进行开箱验货准备。货到指定场所后，采购人及中标单位双方委派代表到现场检查货物外观是否完好，装箱数量、描述与供货清单是否一致，查检无误后双方签署货物签收单，如发现缺漏、外观损坏等，由中标单位负责制定并执行及时的补货换货措施；待中标单位完成补货换货后再由双方代表进行现场查验无误后签署货物签收单。系统试运行期为3个月，如系统在试运行期间发生故障或暴露缺陷，中标单位需进行修复，如3个月内未完成修复，试运行期顺延，直到遗留问题解决。

1. **付款方式**

到货款：主要硬件设备到货，接收单经各方签署以及相关材料齐全，并经招标人第一阶段验收合格后十个工作日内，支付合同总价的20%。

设备安装调试结束，提交全部报告材料，调试完成并经采购人初验合格后十个工作日内，支付合同金额的40%。

项目最终验收合格后十个工作日内，支付合同总价的35%。

验收合格日起满三年后十个工作日内，支付合同总价的5%。

**第五章 政府采购合同主要条款指引**

（具体专用条款由采购人提供）

甲方（采购人）：

乙方（供应商）：

鉴证方：杭州市公共资源交易中心临安分中心

甲、乙双方根据杭州市公共资源交易中心临安分中心关于项目编号为\*\*\*\*\*\*\*\*\*\*的（标项及名称）项目公开招标的结果，签署本合同。

一、货物内容及合同价格

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 采购内容 | 设备性能、型号、配置等 | 品牌 | 单价 | 数量 | 小计 |
|  |  |  |  |  |  |
| 合计 | 小写： | 大写 |  |

注：1、以上表格可自行扩展；商品型号、数量、配置要求等也可附详细清单；

　2、以上合同总价包含产品到达用户并能正常使用所需的一切费用。

二、技术资料

1.乙方应按采购文件规定的时间向甲方提供使用货物的有关技术资料。

2. 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

三、知识产权

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

四、产权担保

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

五、转包或分包

本合同范围的货物，应由乙方直接供应，不得转让他人供应，否则，甲方有权解除合同，没收质量保证金并追究乙方的违约责任。

六、交货期、交货方式及交货地点

1. 交货期：

2. 交货地点：

七、货款支付

 付款方式：

八、税费

本合同执行中相关的一切税费均由乙方负担。

九、质量保证及售后服务

1.乙方保证本合同中所供应的商品是最新生产的符合国家技术规格和质量标准的出厂原装合格产品。如发生所供商品与合同不符，甲方（使用方）有权拒收或退货，由此产生的一切责任和后果由乙方承担。

2. 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

3. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

4.上述的货物在质保期内免费保修，因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

十、调试和验收

1. 甲方对乙方提交的货物依据投标文件上的技术规格要求和国家有关质量标准进行现场验收。货到后，甲方需在五个工作日内验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收。

4. 对技术复杂的货物，甲方应请国家认可的专业检测机构参与验收，并由其出具质量检测报告。

5. 验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由乙方负责。

十一、货物包装

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

十二、违约责任

1. 甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2. 甲方无故逾期验收和办理货款支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3. 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期10个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4. 乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定及投标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

十三、不可抗力事件处理

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

十四、诉讼

双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

十五、合同生效及其它

1. 合同经甲、乙、鉴证方三方签字并加盖单位公章后生效。

2.合同执行中涉及采购资金和采购内容修改或补充的，须经采购中心、财政部门审批，并签书面补充协议，经报政府采购监督管理部门备案后，方可作为主合同不可分割的一部分。

3.采购文件、投标文件与本合同具有同等法律效力。

4.本合同未尽事宜，遵照《合同法》有关条文执行。

5.本合同一式五份，具有同等法律效力，甲、乙方各执二份，鉴证方留存一份。

甲方（盖章）： 乙方（盖章）：

地址： 地址：

法定（授权）代表人： 法定（授权）代表人：

联系电话： 联系电话：

 开户银行及账号：

鉴证方（盖章）：杭州市公共资源交易中心临安分中心

法定（授权）代表人：

 地址：杭州市临安区行政服务中心B座4楼

电话：0571-23616016

传真：0571-23616007 签订时间： 年 月 日

**第六章 投标文件格式**

封面格式正本或副本

\*\*\*项目名称

项目编号：\*\*\*\*\*\*\*\*\*\*\*\*\*\* （标项\*）

**资**

**格**

**文**

**件**

单位全称（公章）：

地 址：

时 间：

**▲**资格部分内容

（1）投标声明书 (格式见附件，含重大违法记录声明)；

（2）提供自招标公告发布之日起至投标截止日内任意时间的“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）投标人信用查询网页截图。（以开标当日采购人或由采购人委托的评标委员会核实的查询结果为准）

（3）法定代表人授权委托书(格式见附件)；

（4）提供有效的营业执照复印件并加盖公司公章；事业单位的，则提供有效的《事业单位法人证书》副本复印件并加盖单位公章；自然人的，则提供有效的身份证复印件并签字；

（5）提供有效的依法缴纳税收证明（完税凭证或税务部门出具的证明）；

（6）提供有效的依法缴纳社会保障资金证明（缴纳凭证或人社部门出具的证明）；

（7）2019年度资产负债表等财务报表资料文件 (或其它财务状况报告，新成立的公司，必须提供情况说明)；

（8）联合投标协议书（若需要）；

（9）联合投标授权委托书（若需要）；

（10）提供采购公告中符合投标人特定条件要求的有效的其他资质复印件并加盖公司公章及需要说明的资料。

**注：以上目录是编制资格文件内容的基本格式要求，投标人可根据自身情况进一步细化。**

**声 明 书**

致杭州市公共资源交易中心临安分中心：

（投标人名称）系中华人民共和国合法企业，经营地址。

我（姓名）系（投标人名称）的法定代表人，我方愿意参加贵方组织的（招标项目名称）（编号为 ）的投标，为此，我方就本次投标有关事项郑重声明如下：

1、我方已详细审查全部招标文件，同意招标文件的各项要求。

2、我方向贵方提交的所有投标文件、资料都是准确的和真实的。

3、若中标，我方将按招标文件规定履行合同责任和义务。

4、我方不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。

5、投标文件自开标日起有效期为90天。

**6、我方参与本项目前3年内的经营活动中没有重大违法记录；**

7、我方通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询，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。

8、以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

法定代表人签名（或签名章）： 日 期：

投标人全称（公章）：

 **法定代表人授权委托书**

（采购机构）：

兹委派我公司 先生/女士(其在本公司的职务是： ，联系电话： 手机： 传真： )，代表我公司全权处理 项目(编号： )政府采购投标的一切事项，若中标则全权代表本公司签订相关合同，并负责处理合同履行等事宜。

 本委托书有效期：自 年 月 日起至 年 月 日止。

特此告知。

 投标人名称(公章)：

 法定代表人(签章)：

签发日期： 年 月 日

 **法定代表人及授权委托人的身份证（复印件）**

**联合投标协议书**

甲方：

乙方：

（如果有的话，可按甲、乙、丙、丁…序列增加）

各方经协商，就响应 组织实施的编号为号的招标活动联合进行投标之事宜，达成如下协议：

一、各方一致决定，以 为主办人进行投标，并按照招标文件的规定分别提交资格文件。

二、在本次投标过程中，主办人的法定代表人或授权代理人根据招标文件规定及投标内容而对招标方和采购人所作的任何合法承诺，包括书面澄清及响应等均对联合投标各方产生约束力。如果中标并签订合同，则联合投标各方将共同履行对招标方和采购人所负有的全部义务并就采购合同约定的事项对采购人承担连带责任。

三、联合投标其余各方保证对主办人为响应本次招标而提供的产品和服务提供全部质量保证及售后服务支持。

四、本次联合投标中，甲方承担的工作和义务为:

乙方承担的工作和义务为：

五、有关本次联合投标的其他事宜：

六、本协议提交招标方后，联合投标各方不得以任何形式对上述实质内容进行修改或撤销。

七、本协议签约各方各持一份，并作为投标文件的一部分。

|  |  |
| --- | --- |
| 甲方单位： （公章）法定代表人： （签章）日 期： 年 月 日 | 乙方单位： （公章）法定代表人： （签章）日 期： 年 月 日 |

**联合投标授权委托书**

 本授权委托书声明：根据 与签订的《联合投标协议书》的内容，主办人的法定代表人现授权 为联合投标代理人，代理人在投标、开标、评标、合同谈判过程中所签署的一切文件和处理与这有关的一切事务， 联合投标各方均予以认可并遵守。

 特此委托。

授权人（签名）：

日期： 年 月 日

授权代表（签名）；

日期： 年 月 日

|  |  |
| --- | --- |
| 联合体甲方单位： （公章）法定代表人： （签章）日 期： 年 月 日 | 联合体乙方单位： （公章）法定代表人： （签章）日 期： 年 月 日 |

 **有效的企业法人营业执照（复印件）**

 **所有资质文件（复印件）**

（由投标人根据采购需求及采购文件自行编制）

|  |  |
| --- | --- |
| **资质要求** | **应标单位具备资质** |
| **必备资质** | **资质级别** | **资质****名称** | **资质****级别** | **颁证****机构** | **证书有效期（起止年月）** | **证书复印件所在页码** | **备注** |
|   |   |  |  |  |  |  |  |
| **其他资质** | **资质级别** | **资质****名称** | **资质****级别** | **颁证****机构** | **证书有效期（起止年月）** | **证书复印件所在页码** | **备注** |
|   |   |  |  |  |  |  |  |
|   |   |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

封面格式正本或副本

\*\*\*项目名称

项目编号：\*\*\*\*\*\*\*\*\*\*\*\*\*\* （标项\*）

**技**

**术**

**及**

**商**

**务**

**文**

**件**

单位全称（公章）：

地 址：

时 间：

▲技术及商务文件响应部分内容

（1）评分对应表（格式见附件，主要用于评委对应评分内容）

（2）投标项目明细清单（含货物、服务等）；

（3）技术响应表（格式见附件）；

（4）项目总体解决方案（可包含且不限于对项目总体要求的理解、项目总体架构及技术解决方案等）；

（5）项目实施计划（可包含且不限于保证工期的施工组织方案及人力资源安排、项目组人员清单等）；

（6）列入政府采购节能环保清单的证明资料（若有）；

（7）商务响应表（格式见附件）；

（8）售后服务计划（可包含且不限于对用户故障的响应、处理、定期巡检、备品备件、常用耗材提供、驻点人员情况等）；

（9）技术培训计划（若有）；

（10）投标人履约能力（可包含且不限于技术力量情况、投标人各项能力证书）；

（11）案例的业绩证明（投标人业绩情况一览表、合同复印件等）；

（12）投标方认为需要的其他文件资料。

**注：以上目录是编制投标技术文件的基本格式要求，各投标人可根据自身情况进一步细化。**

**评分对应表**

投标人全称（公章）： 标项：

|  |  |  |
| --- | --- | --- |
| 评分项目 | 投标文件对应资料 | 投标文件页码 |
| 对应第三章评分办法及评分标准（报价除外） |  |  |
| …… |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

授权代表签名： 日期：

**投标项目明细清单**

投标人全称（公章）： 标项：

货物类

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 品牌 | 规格型号 | 单位及数量 | 性能及指标 | 产地 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

服务类

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务内容 | 服务人员数量 | 工作量 |
|  |  |  |  |
|  |  |  |  |

注：在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。

授权代表签名： 日期：

**技 术 响 应 表**

投标人全称（公章）： 标项：

|  |  |  |
| --- | --- | --- |
| 招标文件要求 | 投标文件响应 | 偏离情况  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

注：投标人应根据投标设备的性能指标、对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

授权代表签名： 日 期：

**项目组人员清单**

投标人全称（公章）： 标项：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 姓名 | 职务 | 专业技术资格 | 证书编号 | 参加本单位工作时间 | 劳动合同编号 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

授权代表签名： 日 期：

**商务响应表**

投标人全称（公章）： 标项：

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 招标文件要求 | 是否响应 | 投标人的承诺或说明 |
| 供货时间（项目工期）及地点 |  |  |  |
| 付款条件 |  |  |  |
| 违约责任及争议解决方式 |  |  |  |
| 项目维护计划 |  |  |  |
| 响应情况 |  |  |  |
| 本地化服务要求 |  |  |  |
| 技术培训 |  |  |  |
| 公司技术力量情况 |  |  |  |
| 经验或业绩要求 |  |  |  |
| …… |  |  |  |

授权代表签名： 日期：

**投标人业绩情况一览表**

投标人全称（公章）：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 采购单位名称 | 设备或项目名称 | 采购数量 | 单价 | 合同金额（万元） | 附件页码 | 采购单位联系人及联系电话 |
| 合同 | 验收报告 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 备注 | 提供投标人同类项目合同复印件、用户验收报告（如有）。 |

授权代表签名：

封面格式正本或副本

\*\*\*项目名称

项目编号：\*\*\*\*\*\*\*\*\*\*\*\*\*\* （标项\*）

**报**

**价**

**文**

**件**

单位全称（公章）：

地 址：

时 间：

▲报价文件

（1）开标一览表（报价表）

（2）投标报价明细表（见附件）；

（3）小微企业声明函（见附件）；

（4）残疾人福利企业声明函（见附件）；

（5）小微企业名录查询记录

（6）投标人针对报价需要说明的其他文件和说明（格式自拟）。

**开标一览表（报价表）**

单位全称（公章）： 项目编号：

|  |  |  |  |
| --- | --- | --- | --- |
| 项目名称 | 数量 | 投标报价 | 备注 |
|  |  |  |  |

注: 1、此表报价单不得涂改，请按规定要求填报。

2、以上报价应与“报价明细表”中的“合计”数相一致。

3、项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、购买及制作标书费、税费及其他一切费用。

全权代表（签字）： 日 期：

**报 价 明 细 表**

单位全称（公章）：

|  |
| --- |
| **货物类** |
| **货物****名称** | **品牌** | **产地** | **规格****型号** | **数量** | **单价****（元）** | **总价（元）** | **制造商情况** |
| **是否小微企业** | **企业全称** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |  |  |
| **小微企业价格合计金额大写： 小写： ￥** |
| **投标总价合计金额大写： 小写： ￥** |
| 备注 | 1、此表应按项目的明细情况列项填报,在填写时，如上表不适合本项目的实际情况，可在确保投标明细内容完整的情况下，根据上表格式自行划表填写。2、报价要求：项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、税费及其他一切费用。3、报价中不允许出现报价优惠等字样,投标总价合计金额应与明细报价汇总相等。**4、小微企业价格合计金额应与“制造商为小微企业”的明细报价汇总相等（如有错误修正，以修正后的明细报价为准），评标委员会按前附表“小微企业有关政策”要求对小微企业价格进行确认，并对符合要求的小微企业价格部分给予价格扣除。**5**、**开标时，现场工作人员当众拆封，并宣布投标人名称、投标总价合计金额。 |

全权代表签名： 日 期：

**小微企业声明函**

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181号）的规定，本公司为（请填写：小型、微型）企业。即，本公司同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）规定的划分标准，本公司为（请填写：小型、微型）企业。

2.本公司参加单位的项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他（请填写：小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

 日 期：

**残疾人福利性单位声明函**

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加\_\_\_\_\_\_单位的\_\_\_\_\_\_项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

 单位名称（盖章）：

 日 期：

“国家企业信用信息公示系统——小微企业名录”页面查询结果

附表：

政府采购融资畅通工程金融机构联系信息表

|  |  |  |  |
| --- | --- | --- | --- |
| 金融机构各称 | 联系人 | 联系电话 | 联系地址 |
| 南浔银行 | 方薇 | 13868003773 | 城中街638号 |
| 浦发银行临安分行 | 沈丹丹 | 6109293613777851690 | 钱王大街417号 |
| 杭州银行临安支行 | 金林妹 | 13666638571 | 万马路255号 |
| 临安中信村镇银行 | 吕祎 | 13787100002 61109033 | 石镜街777号 |