**柯城区县域医共体建设-2021年基层医疗机构整体提升工程柯城区人民医院信息化提升工程**

公 开 招 标 文 件

(电子标)

项目编号：HBMDCG2021-055

|  |  |
| --- | --- |
| 采购人： | 衢州市柯城区卫生健康局  |
| 采购代理机构： | 湖北名达工程咨询有限责任公司 |
|  |  |
| 二○二一年十月 |

**目 录**

第一部分 招标公告

第二部分 投标人须知

第三部分 采购需求

第四部分 评标方法及评分标准

第五部分 拟签订的合同文本

第六部分 应提交的有关格式范例

**第一部分 招标公告**

|  |
| --- |
| 项目概况  柯城区县域医共体建设-2021年基层医疗机构整体提升工程柯城区人民医院信息化提升工程的潜在供应商应在浙江政府采购网本项目公告附件获取（下载）招标文件，并于2021年 11月5 日 14 : 30 （北京时间）前提交（上传）响应文件。    |

## 一、项目基本情况

项目编号：HBMDCG2021-055

项目名称：柯城区县域医共体建设-2021年基层医疗机构整体提升工程柯城区人民医院信息化提升工程

预算金额（元）： 5500000

最高限价（元）： 4733460

采购需求：

标项一
    标项名称: 柯城区县域医共体建设-2021年基层医疗机构整体提升工程柯城区人民医院信息化提升工程
    数量: 1
    预算金额（元）: 5500000
    简要规格描述或项目基本概况介绍、用途：详见招标文件第三部分采购需求。

    备注：无

合同履行期限：中标人应在合同签订之日起15日历天内完成供货，供货后15日历天内完成安装、调试并验收合格。

本项目（否）接受联合体投标。

## 二、申请人的资格要求：

满足《中华人民共和国政府采购法》第二十二条规定；

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。

落实政府采购政策需满足的资格要求：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的声明。 具有良好商业信誉的特别声明. 供应商为中小企业/小微企业。

本项目的特定资格要求：无

## 三、获取招标文件

时间：/至2021年11月5日，每天上午00:00至12:00，下午12:00至23:59（北京时间，线上获取法定节假日均可，线下获取文件法定节假日除外）

地点（网址）：政采云平台（<https://www.zcygov.cn/>）

方式：供应商登录政采云平台https://www.zcygov.cn/在线申请获取招标文件（进入“项目采购”应用，在获取招标文件菜单中选择项目，申请获取招标文件）

    售价（元）：0

## 四、提交投标文件截止时间、开标时间和地点

**提交投标文件截止时间：**2021年11月5日 14点30分00秒（北京时间）

**开标时间：**2021年11月 5日 14点30分00秒

**开标地点：**政采云平台/衢州市柯城区住建局四楼开标厅。

## 五、公告期限

自本公告发布之日起5个工作日。

## 六、其他补充事宜

1、供应商认为招标文件使自己的权益受到损害的，可以自获取招标文件之日或者招标文件公告期限届满之日（公告期限届满后获取招标文件的，以公告期限届满之日为准）起7个工作日内，以书面形式向采购人和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。

 2、其他事项：本项目对符合财政扶持政策的中小企业（小型、微型）、监狱企业、残疾人福利性单位给予价格优惠扶持，执行节能产品政府强制采购和优先采购政策，执行环境标志产品政府优先采购政策。采购项目需要落实的政府采购政策：《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）、《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）、《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）、《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》财库〔2019〕9号。

3、政府采购金融服务：鼓励供应商开展政采贷【通过政府采购云平台（http://www.zcygov.cn/）首页的“金融服务”模块进入申请】、履约保函等政府采购金融服务，供应商可以银行、保险公司出具保函形式提交履约保证金。

## 七、对本次招标提出询问，请按以下方式联系。

1.采购人信息

名 称：衢州市柯城区卫生健康局

地址：浙江省衢州市柯城区荷三路231号

传真：/

项目联系人（询问）：王老师

项目联系方式（询问）：0570-3085367

质疑联系人：王老师

质疑联系方式：0570-3085367

2.采购代理机构信息

名 称：湖北名达工程咨询有限责任公司

地址：衢州市柯城区书院西路63号

传真：/

项目联系人（询问）：李刚

项目联系方式（询问）：15257038663

质疑联系人：徐利军

质疑联系方式：13255818663

3.同级政府采购监督管理部门

名称：衢州市柯城区政府采购管理办公室

地址：/

传真：/

联系人 ：蒋先生

监督投诉电话： 0570-3028506

若对项目采购电子交易系统操作有疑问，可登录政采云（https://www.zcygov.cn/），点击右侧咨询小采，获取采小蜜智能服务管家帮助，或拨打政采云服务热线400-881-7190获取热线服务帮助。

CA问题联系电话（人工）：汇信CA 400-888-4636；天谷CA 400-087-8198。

**第二部分 投标人须知**

**前附表**

| **序号** | **事项** | **内 容** |
| --- | --- | --- |
| 1 | 采购项目 | 项目名称：柯城区县域医共体建设-2021年基层医疗机构整体提升工程柯城区人民医院信息化提升工程；项目编号：HBMDCG2021-055；项目要求：详见第三部分“采购需求”。 |
| 2 | 采购方式 | 公开招标。 |
| 3 | 投标人资格要求 | 详见公开招标公告。 |
| 4 | 投标文件组成 | 包含资格证明文件、资信技术文件一份、报价文件一份。本项目实行网上投标，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。注明：供应商需自行准备电脑和制作标书的CA锁。 |
| 5 | 投标有效期 | 自投标截止日起90天。 |
| 6 | 递交投标文件截止时间与递交地点 | 截止时间：2021年 11 月5日 14 :30分。递交地点：政采云平台 |
| 7 | 开标时间与地点 | 时间：2021年 11月5日 14:30分。地点：政采云平台/衢州市柯城区住建局四楼开标厅。 |
| 8 | 投标保证金 | 无 |
| 9 | 履约保证金 | 中标人在签订合同时缴纳履约保证金，履约保证金金额为中标价的3%，履约保证金可以转账、保函等形式缴纳。合同开始履行，项目验收合格后转为质保金，在正常使用一年后退还中标人。 |
| 10 | 分包或转包。 | （1）本项目不得分包（2）本项目不得转包。 |
| 16 | 同级采购监督管理部门 | 衢州市柯城区政府采购管理办公室 联系人 ：蒋先生  监督投诉电话：0570-3028506 |
| 17 | 服务费 | 1、代理费、评委费、专家费按实收取。2、结算方式及时间为：在领取中标通知书时由中标人一次性向采购代理机构付清。3、以上费用均不在报价中单列，请投标人在报价中予以考虑 |
| 18 | 其他 | 无 |

**注：本项目通用总则条款与前附表等专用特别规定有冲突之处，以专用条款（特别规定）为准。**

**一、总则**

**1. 适用范围**

本招标文件适用于该项目的招标、投标、开标、资格审查及信用信息查询、评标、定标、合同、验收等行为（法律、法规另有规定的，从其规定）。

 **2.定义**

2.1 “采购人”系指招标公告中载明的本项目的采购人。

2.2 “采购机构”系指招标公告中载明的本项目的采购机构。

2.3 “投标人”系指是指响应招标、参加投标竞争的法人、其他组织或者自然人。。

2.4 “负责人”系指法人企业的法定负责人，或其他组织为法律、行政法规规定代表单位行使职权的主要负责人，或自然人本人。

2.5 “▲”系指实质性要求条款，“★”系产品采购项目中单一产品或核心产品。

**3.采购项目需要落实的政府采购政策**

3.1本项目原则上采购本国生产的货物、工程和服务，不允许采购进口产品。除非采购人采购进口产品，已经在采购活动开始前向财政部门提出申请并获得财政部门审核同意，且在采购需求中明确规定可以采购进口产品（但如果因信息不对称等原因，仍有满足需求的国内产品要求参与采购竞争的，采购人、采购机构不会对其加以限制，仍将按照公平竞争原则实施采购）。

3.2支持中小企业发展。

3.2.1中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。

符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。

3.2.2在政府采购活动中，投标人提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。

在货物采购项目中，投标人提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。

以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

3.2.2对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，采购人、采购代理机构应当对符合本办法规

定的小微企业报价给予 6%（工程项目为 3%）的扣除，用扣除后的价格参加评审。适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，评标时应当在采用原报价进行评分的基础上增加其价格得分的3%作为其价格分。

3.2.3接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的，采购人、采购代理机构应当对联合体或者大中型企业的报价给予 2%（工程项目为 1%）的扣除，用扣除后的价格参加评审。适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，评标时应当在采用原报价进行评分的基础上增加其价格得分的 1%作为其价格分。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

3.2.4符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件1）的残疾人福利性单位视同小型、微型企业；

3.2.5符合《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）规定的监狱企业并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证明文件的，视同为小型、微型企业。

3.2.6可享受中小企业扶持政策的投标人应按照招标文件格式要求提供《中小企业声明函》。

3.2.7中小企业享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

**4. 询问、质疑、投诉**

4.1供应商询问

供应商可以就招标文件中特定资格条件、采购需求、评分办法及采购过程中有关现场考察或开标前答疑会事项向采购人提出询问，采购人将对此作出答复；供应商可以就采购活动 中的其它事项向采购机构提出询问，采购机构将对此作出答复。答复的内容不得涉及商业秘密。

4.2供应商质疑

4.2.1提出质疑的供应商应当是参与所质疑项目采购活动的供应商。潜在供应商已依法获取其可质疑的招标文件的，可以对该文件提出质疑。

4.2.2供应商认为招标文件、采购过程和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七个工作日内，以书面形式向采购人或者采购机构提出质疑，否则，采购人或者采购机构不予受理：

4.2.2.1对招标文件提出质疑的，质疑期限为供应商获得招标文件之日或者招标文件公告期限届满之日起计算。招标文件在获取截止之日后获得的，应当自招标文件公告期限届满之日起计算，且应当在采购响应截止时间之前提出。对招标文件中特定资格条件、采购需求、评分办法提出的质疑，由采购人负责答复；对招标文件中其他内容提出的质疑，由采购机构负责答复。

4.2.2.2对采购过程提出质疑的，质疑期限为各采购程序环节结束之日起计算。对同一采购程序环节的质疑，供应商须一次性提出。对采购过程中有关现场考察或开标前答疑会事项提出的质疑，由采购人负责答复；对采购过程中其它事项提出的质疑，由采购机构负责答复。

4.2.2.3对采购结果提出质疑的，质疑期限自采购结果公告期限届满之日起计算。对采购结果提出质疑的，采购人或采购机构负责答复。（详见前附表相关规定）

4.2.3供应商提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

　　4.2.3.1供应商的姓名或者名称、地址、邮编、联系人及联系电话；

　　4.2.3.2质疑项目的名称、编号；

　　4.2.3.3具体、明确的质疑事项和与质疑事项相关的请求；

　　4.2.3.4事实依据；

　　4.2.3.5必要的法律依据；

4.2.3.6提出质疑的日期。

供应商提交的质疑函需一式三份。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

质疑函范本及制作说明详见附件2。

4.2.4采购人或者采购机构应当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与质疑处理结果有利害关系的政府采购当事人，但答复的内容不得涉及商业秘密。

4.2.5询问或者质疑事项可能影响采购结果的，采购人应当暂停签订合同，已经签订合同的，应当中止履行合同。

4.2.6质疑接收人：详见前附表

4.3供应商投诉

4.3.1质疑供应商对采购人、采购机构的答复不满意或者采购人、采购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提出投诉。

4.3.2供应商投诉的事项不得超出已质疑事项的范围，基于质疑答复内容提出的投诉事项除外。

4.3.3供应商投诉应当有明确的请求和必要的证明材料。

4.3.5 以联合体形式参加政府采购活动的，其投诉应当由组成联合体的所有供应商共同提出。

投诉书范本及制作说明详见附件3。

**二、招标文件的构成、澄清、修改**

**5．招标文件的构成**

5.1 招标文件包括下列文件及附件

* 第一部分 招标公告
* 第二部分 投标人须知
* 第三部分 采购需求
* 第四部分 评标方法及评分标准
* 第五部分 拟签订的合同文本
* 第六部分 应提交的有关格式范例

5.2与本项目有关的澄清或者修改等公告、内容亦为招标文件的组成部分，投标人须自行于招标公告所在网站获取相关信息（浙江政府采购网网址http://zfcg.czt.zj.gov.cn/）。

**6. 招标文件的澄清、修改**

6.1已获取招标文件的潜在投标人，若有问题需要澄清，应于投标截止时间前，以书面形式向采购机构提出，采购机构与采购人研究后，对认为有必要回答的问题，将以公告形式通知所有招标文件收受人。

6.2采购机构如对已发出的招标文件进行必要澄清或者修改的，将在发布招标公告的网站上发布更正、补遗公告，同时视情况延长投标截止时间和开标时间。该公告澄清或者修改的内容为招标文件的组成部分。

**▲投标文件未按招标文件更正、补遗公告的澄清、修改的内容编制，又不符合实质性要求的，投标无效。**

**三、投标**

**7.招标文件的获取**

详见招标公告中获取招标文件的时间期限、地点、方式。附件中直接下载仅供浏览使用。

**▲未按照公告要求完成招标文件获取的，投标无效。**

**8.开标前答疑会或现场考察**

采购人视采购项目的具体情况，如果采购人组织潜在投标人现场考察或者召开开标前答疑会的，潜在投标人按前附表的规定参加现场考察或者开标前答疑会。**采购人不单独或分别组织只有一个供应商参加的现场考察和答疑会。**

**本项目不组织。**

**9.投标保证金**

本项目不收取投标保证金。

**10. 投标文件的语言**

投标文件及投标人与采购有关的来往通知、函件和文件均应使用中文。

**11. 投标文件的组成**

投标文件应当包括以下主要内容：**资格文件、报价文件、资信技术文件**。投标文件应当对招标文件提出的要求和条件作出明确响应。

11.1**资格文件**应包括以下内容（均需使用电子签章）：证明其符合《中华人民共和国政府采购法》规定的供应商基本条件和采购项目对供应商的特定条件（如果项目要求）的有关资格证明文件。**（以联合体形式进行政府采购的，参加联合体的供应商均应当提供）**

11.1.1营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，提供自然人的身份证明）、税务登记证(或其它依法缴纳税收的相关材料)复印件、社保登记证（或其它依法缴纳社会保障资金的相关材料）复印件；实施“多证合一、一照一码”登记制度改革的，只需提供改革后取得的营业执照复印件；

金融、保险、通讯等特定行业的全国性企业所设立的区域性分支机构，以及个体工商户、个人独资企业、合伙企业，如果已经依法办理了工商、税务和社保登记手续，并且获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料（在投标文件中提供相关材料），证明其具备实际承担责任的能力和法定的缔结合同能力，可以独立参加政府采购活动，由单位负责人签署相关文件材料；

11.1.2 最近一年度资产负债表或审计报告等财务报表资料文件 (新成立的公司，必须提供情况说明)；

11.1.3具有履行合同所必需的设备和专业技术能力的承诺函；

11.1.4参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的声明；

11.1.5具有良好商业信誉的特别声明；

11.1.6授权书（如法定代表人直接参加投标并对相应文件签字的，只需提供其身份证复印件正反面；如以联合体形式参加政府采购活动的，按招标文件有关格式范例提供联合体投标授权书）。

11.2 投标人的**报价文件**应包括以下内容（均需使用电子签章）：

11.2.1投标响应函；

11.2.2投标(开标)一览表；

11.2.3中小企业声明函。

11.3 投标人的**资信技术文件应**包括以下内容（均需使用电子签章）：

11.3.1营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，须提供自然人的身份证明）；

11.3.2法定代表人授权书，法定代表人及其授权代表的身份证复印件（正反面复印件）；如法定代表人直接参加投标并对相应文件签字的，只需提供其身份证复印件（正反面复印件）；▲**投标文件中法定代表人授权书所载内容与本项目内容有异的，投标无效。**

11.3.3如以联合体形式参加政府采购活动的，联合体各方应当指定牵头人，授权其代表所有联合体成员负责投标和合同实施阶段的主办、协调工作，并应当向采购机构提交由所有联合体成员各方法定代表人签署的授权书，同时应当提交联合协议，载明联合体各方承担的工作和义务。联合体协议中应当注明由联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。联合体协议中仅约定由牵头人或联合体成员中某一方与采购人签订合同的，或联合体协议中仅约定由牵头人或联合体成员中某一方就采购合同约定的事项对采购人承担责任的，视为联合体协议不成立，该联合体投标文件将被作无效投标文件处理；（**▲如以联合体形式参加政府采购活动的，联合体协议不符合招标文件规定的联合体协议要求的，投标无效。**）

11.3.4投标截止时间前三年投标人的主要业绩证明材料即合同；

11.3.5资信文件：见投标须知前附表所述；

11.3.6 资信技术评分中涉及的内容；

11.3.7投标人认为需要的其他商务文件或说明；

11.3.8关于对招标文件商务、合同中有关条款的拒绝声明。（如果有）

**▲投标文件组成漏项，内容不全或内容字迹模糊辨认不清的，投标无效；**

**▲投标文件含有采购人不能接受的附加条件的，投标无效；**

**▲投标人提供虚假材料投标的，投标无效。**

**▲根据法律、法规或招标文件要求，评标委员会认为应当作无效投标的其他情况。**

**12. 投标文件的编制**

12.1投标文件分为资格文件、资信技术文件、报价文件三部分。各投标人在编制投标文件时请按照招标文件第六部分规定的格式进行，混乱的编排导致投标文件被误读或评标委员会查找不到有效文件是投标人的风险。

12.2投标人进行电子投标应安装客户端软件—“政采云电子交易客户端”，并按照招标文件和电子交易平台的要求编制并加密投标文件。投标人未按规定加密的投标文件，电子交易平台将拒收并提示。

12.3使用“政采云电子交易客户端”需要提前申领CA数字证书，申领流程请自行前往“浙江政府采购网-下载专区-电子交易客户端-CA驱动和申领流程”进行查阅。

**13.投标文件的签署、盖章**

13.1投标文件按照招标文件第六部分格式要求进行签署、盖章。**投标人的投标文件未按照招标文件要求签署、盖章的，其投标无效**。

13.2为确保网上操作合法、有效和安全，投标人应当在投标截止时间前完成在“政府采购云平台”的身份认证，确保在电子投标过程中能够对相关数据电文进行加密和使用电子签章。

**14.投标文件的提交、补充、修改、撤回**

14.1 供应商应当在投标截止时间前完成投标文件的传输递交，并可以补充、修改或者撤回投标文件。补充或者修改投标文件的，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。投标截止时间后递交的投标文件，电子交易平台将拒收。

14.2电子交易平台收到投标文件，将妥善保存并即时向供应商发出确认回执通知。在投标截止时间前，除供应商补充、修改或者撤回投标文件外，任何单位和个人不得解密或提取投标文件。

14.3采购机构可以视情况延长投标文件提交的截止时间。在上述情况下，采购机构与投标人以前在投标截止期方面的全部权利、责任和义务，将适用于延长至新的投标截止期。

**15. 备份投标文件以及投标文件的递交**

15.1电子备份投标文件须在“政采云投标客户端”制作生成，并储存在U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(联合体投标的，包装物封面需注明联合体投标，并注明联合体成员各方的名称和联合体协议中约定的牵头人的名称)

**▲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。**

15.4 供应商应当在投标截止时间前完成投标文件的传输递交，并可以补充、修改或者撤回投标文件。补充或者修改投标文件的，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。投标截止时间后递交的投标文件，电子交易平台将拒收。

15.5采购机构可以视情况延长投标文件提交的截止时间。在上述情况下，采购机构与投标人以前在投标截止期方面的全部权利、责任和义务，将适用于延长至新的投标截止期。

15.6如项目须备份投标文件，投标人应按“招标公告”及前附表规定的时间、地点完成招标文件获取手续并将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投标文件和未按公告要求完成招标文件获取的投标人递交的投标文件。

**16.投标文件的无效处理**

有招标文件第四部分第13项规定的情形之一的，投标无效：

**17.投标有效期**

17.1投标有效期为从提交投标文件的截止之日起90天。▲**投标人的投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的，投标无效。**

17.2投标文件合格投递后，自投标截止日期起，在投标有效期内有效。

17.3在原定投标有效期满之前，如果出现特殊情况，采购机构可以以公告形式通知投标人延长投标有效期。投标人同意延长的，不得要求或被允许修改其投标文件，投标人拒绝延长的，其投标无效。

**四、开标、资格审查与信用信息查询**

**18.开标**

18.1采购机构按照招标文件规定的时间通过电子交易平台组织开标，所有投标人均应当准时在线参加。投标人不足3家的，不得开标。

18.2开标时，电子交易平台按开标时间自动提取所有投标文件。采购机构依托电子交易平台发起开始解密指令，投标人按照平台提示和招标文件的规定在半小时内完成在线解密。

18.3项目允许提供备份文件时，仅因政采云平台或CA原因无法读取或电子开评标无法正常进行，采购代理将按顺序启用备份文件完成开标。投标人因自身原因（不会使用、使用不当等）未按时完成解密的，投标无效，不启用备份文件。**投标文件已按时解密的，备份投标文件自动失效。**

18.4 备份投标文件的接收在招标文件确定的时间、地点进行。

**19、资格审查**

19.1开标后，采购人将依法对投标人的资格进行审查。

19.2采购人或采购机构依据法律法规和招标文件的规定，对投标人的基本资格条件、特定资格条件进行审查。

19.3投标人未按照招标文件要求提供与基本资格条件、特定资格条件相应的有效资格证明材料的，视为投标人不具备招标文件中规定的资格要求，其投标无效。

19.4对未通过资格审查的投标人，采购人或采购机构告知其未通过的原因。

19.5合格投标人不足3家的，不再评标。

**20、信用信息查询**

20.1信用信息查询渠道及截止时间：采购人或采购机构将通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道查询投标人投标截止时间前的信用记录。

20.2信用信息查询记录和证据留存的具体方式：现场查询的投标人的信用记录、查询结果经确认后将与招标文件一起存档。

20.3信用信息的使用规则：经查询列入失信被执行人名单、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投标人将被拒绝参与政府采购活动。

20.4联合体信用信息查询：两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，应当对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

**五、评标**

**21.1评标委员会**

评标由采购人代表和评审专家组成，成员人数5人。

**21.2评标**

评标委员会按照第三章“评标标准和方法”规定的方法、评审因素、标准和程序对投标文件进行评审。第三章“评标标准和方法”没有规定的方法、评审因素和标准，不作为评标依据。

**六、定 标**

**22. 确定中标供应商**

采购机构将自评审结束之日起2个工作日内将评审报告送交采购人。采购人将自收到评审报告之日起5个工作日内在评审报告推荐的中标候选人中按顺序确定中标供应商。

**23. 中标通知与中标结果公告**

25.1采购机构将在自中标人确定之日起2个工作日内，发布招标公告的网站上公告中标结果，同时发出中标通知书。

25.2中标结果公告内容包括采购人及其委托的采购机构的名称、地址、联系方式，项目名称和项目编号，中标人名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求，中标公告期限以及评审专家名单。

25.3公告期限为1个工作日。

**七、合同授予**

**24.** 合同主要条款详见第五部分拟签订的合同文本。

**25. 合同的签订**

25.1 采购人与中标人应当在中标通知书发出之日起三个工作日内，按照招标文件确定的事项双方签订政府采购合同。

25.2中标人按规定的日期、时间、地点，由法定代表人或其授权代表与采购人代表签订合同。如中标人为联合体的，由联合体成员各方法定代表人或其授权代表与采购人代表签订合同。

25.3如签订合同并生效后，供应商无故拒绝或延期，除按照合同条款处理外，列入不良行为记录一次，并给予通报。

25.4中标供应商拒绝或逾期与采购人签订合同的，采购人可以按照评审报告推荐的中标或者成交候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

**26. 履约保证金**

拟签订的合同文本要求中标供应商提交履约保证金的，供应商应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。履约保证金的数额不得超过政府采购合同金额的3%。

**八、电子交易活动的中止**

**27. 电子交易活动的中止。**采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购机构可中止电子交易活动：

29.1电子交易平台发生故障而无法登录访问的；

29.2电子交易平台应用或数据库出现错误，不能进行正常操作的；

29.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

29.4病毒发作导致不能进行正常操作的；

29.5其他无法保证电子交易的公平、公正和安全的情况。

出现以上情形，不影响采购公平、公正性的，采购组织机构可以待上述情形消除后继续组织电子交易活动；影响或可能影响采购公平、公正性的，应当重新采购。

**第三部分 采购需求**

“▲”标明的属于实质性要求条款，“★”标明的属于核心技术参数。

一、设备清单

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **数量** |
| **1** | **虚拟化服务器** | **12台** |
| **2** | **数据库服务器** | **4台** |
| **3** | **虚拟化存储** | **2台** |
| **4** | **PACS存储** | **1台** |
| **5** | **备份一体机** | **1套** |
| **6** | **光纤交换机** | **2台** |
| **7** | **WEB应用防火墙（WAF）** | **1台** |
| **8** | **堡垒机** | **1台** |
| **9** | **内网专线防火墙** | **2台** |
| **10** | **网闸** | **1台** |
| **11** | **态势感知** | **1套** |
| **12** | **数据脱敏** | **1台** |
| **13** | **上网行为管理**  | **1台** |
| **14** | **VPN** | **1台** |
| **15** | **综合运维管理平台** | **1套** |
| **16** | **精密空调** | **2台** |
| **17** | **数据中心系统割接迁移和机房设施** | **1批** |

二、技术规范和功能要求

（一）虚拟化服务器

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 品牌 | 业界知名品牌 |
| 投标机型在官方网站中文资料齐全，包含中文版（产品彩页、规格白皮书、兼容性列表、用户指南、安装升级指南等）。 |
| 2 | 规格 | ≤2U |
| 3 | ▲CPU | 支持Intel® Xeon® Scalable Processors (TDP up to 205W)系列处理器 |
| 实配两路CPU，主频:≥2.1GHz，≥20核 |
| 4 | 内存 | 内存类型：ECC DDR4 RDIMM/LRDIMM内存插槽内存槽位 最大支持 24个 |
| ▲内存配置容量：≥512GB |
| 故障DIMM标识隔离（Failed DIMM Isolation）单颗粒数据纠错（SDDC）内存巡检（Memory Demand and Patrol Scrubbing）内存地址奇偶检测保护（Memory Address Parity Protection）内存过热调节（Memory Thermal Throttling）内存Rank冗余热备（Memory Sparing）内存镜像（Memory Mirroring）设备标记（Device Tagging）数据加扰（Data Scrambling），提供官网证明材料。 |
| 5 | 存储 | 内置硬盘类型：热插拔SAS/SATA/SSD硬盘 |
| 内置硬盘配置数目：≥2块600GB SAS硬盘' |
| 配置磁盘阵列卡，缓存≥2G，支持RAID 0/1/10/5/50/6/60 |
| 6 | 内置存储 | 支持 2\*M.2 SATA SSD，支持硬RAID1，支持免开箱热插拔 |
| 7 | 网口和光纤卡 | 配置：4\*GE+2\*10GE（配置光模块）+2\*16GB FC（配置光模块） |
| 8 | 环境温度  | 长期工作环境温度支持 5-45度，提供官网材料证明 |
| 9 | 可管理性 | 投标产品支持Redfish标准提供RESTful接口，投标厂商需要提供证明材料。 |
| 投标产品单板管理软件的Firmware支持双镜像，主引导区升级失效，可以从从引导区启动。投标厂商需要提供白皮书，官网证明材料。 |
| 投标产品支持使用客户端证书和证书密码的双因素认证方式登录单板管理系统。投标厂商需要提供白皮书，官网证明材料。 |
| 投标产品具备带外故障检测功能，不依赖于OS，对CPU故障；I2C和 IPMB总线故障；内存故障；硬盘故障，系统宕机、黑屏、蓝屏和异常重启故障等进行分析和定位。投标厂商需要提供白皮书，官网证明材料。 |
| 带内外融合管理 |
| 10 | ★BIOS | 支持中文BIOS界面，提供官网证明材料 |
| 投标产品支持支持图形化界面，支持鼠标操作。投标厂商需要提供白皮书，官网证明材料。 |
| 11 | 产品资质 | 中国环境标志产品认证证书（中国）提供证书证明 |
| 中国CQC节能认证提供证书证明 |
| 12 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

（二）数据库服务器

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 品牌 | 业界知名品牌 |
| 投标机型在官方网站中文资料齐全，包含中文版（产品彩页、规格白皮书、兼容性列表、用户指南、安装升级指南等）。 |
| 2 | 规格 | ≤2U |
| 3 | ▲CPU | 支持Intel® Xeon® Scalable Processors (TDP up to 205W)系列处理器 |
| 实配两路INTEL 6系CPU，主频:≥2.1GHz，≥16核 |
| 4 | 内存 | 内存类型：ECC DDR4 RDIMM/LRDIMM内存插槽内存槽位 最大支持 24个 |
| ▲内存配置容量：≥512GB |
| 故障DIMM标识隔离（Failed DIMM Isolation）单颗粒数据纠错（SDDC）内存巡检（Memory Demand and Patrol Scrubbing）内存地址奇偶检测保护（Memory Address Parity Protection）内存过热调节（Memory Thermal Throttling）内存Rank冗余热备（Memory Sparing）内存镜像（Memory Mirroring）设备标记（Device Tagging）数据加扰（Data Scrambling），提供官网证明材料。 |
| 5 | 存储 | 内置硬盘类型：热插拔SAS/SATA/SSD硬盘 |
| 内置硬盘配置数目：≥2块600GB SAS硬盘' |
| 配置磁盘阵列卡，缓存≥2G，支持RAID 0/1/10/5/50/6/60 |
| 6 | 内置存储 | 支持 2\*M.2 SATA SSD，支持硬RAID1，支持免开箱热插拔 |
| 7 | 网口和光纤卡 | 配置：4\*GE+2\*10GE（配置光模块）+2\*16GB FC（配置光模块） |
| 8 | 环境温度  | 长期工作环境温度支持 5-45度，提供官网材料证明 |
| 9 | 可管理性 | 投标产品支持Redfish标准提供RESTful接口，投标厂商需要提供证明材料。 |
| 投标产品单板管理软件的Firmware支持双镜像，主引导区升级失效，可以从从引导区启动。投标厂商需要提供白皮书，官网证明材料。 |
| 投标产品支持使用客户端证书和证书密码的双因素认证方式登录单板管理系统。投标厂商需要提供白皮书，官网证明材料。 |
| 投标产品具备带外故障检测功能，不依赖于OS，对CPU故障；I2C和 IPMB总线故障；内存故障；硬盘故障，系统宕机、黑屏、蓝屏和异常重启故障等进行分析和定位。投标厂商需要提供白皮书，官网证明材料。 |
| 带内外融合管理 |
| 10 | ★BIOS | 支持中文BIOS界面，提供官网证明材料 |
| 投标产品支持支持图形化界面，支持鼠标操作。投标厂商需要提供白皮书，官网证明材料。 |
| 11 | 产品资质 | 中国环境标志产品认证证书（中国）提供证书证明 |
| 中国CQC节能认证提供证书证明 |
| 12 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 虚拟化存储

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类别** | **指标项** | **指标要求** |
|  | 架构 | 体系架构 | 2个控制器采用Active-Active架构，LUN不归属于某一个控制器，业务负载均衡到所有控制器，并提供具备CNAS(中国合格评定国家认可委员会)资质的第三方权威评测机构签字盖章的测试报告，加盖投标人有效印章 |
| 协议融合 | SAN和NAS一体化，配置NAS协议（包括NFS和CIFS）、IP SAN和FC SAN协议，不需额外配置NAS网关，提供官网证明截图 |
| ▲前后端架构 | 全闪存，前端采用基于FC或者RDMA的NVMe协议，后端支持基于RDMA的NVMe协议，支持端到端NVMe架构； |
| 控制器扩展能力 | 支持控制器扩展，最大支持≥8控 |
|  | 时延 | 稳定时延≤0.5ms，包括开启增值功能的情况下，包括开启快照等功能(不少于3个)并提供具备CNAS(中国合格评定国家认可委员会)资质的第三方权威评测机构签字盖章的测试报告 |
|  | 配置 | 控制器处理器 | 采用多核处理器，配置控制器处理器总物理核心数≥32核，提供官网处理器核数截图及链接 |
| ▲存储缓存容量 | 系统内总一级缓存容量配置≥256GB，且任意控制器一级缓存容量≥128GB（不含任何性能加速模块、FlashCache、PAM卡，SSD Cache、SCM等）控制器缓存均具备断电保护功能，在出现电源故障时，可提供充足的电源，将高速缓存内容转储至非易失性内部存储设备上（非通用服务器架构） |
| 前端主机通道接口 | 可支持配置8/16/32G FC，10/25/40/100 GE支持配置8\*16Gbps FC接口，支持FC-NVMe（满配多模光模块），支持配置：8\*10Gbps Ethernet接口；（满配多模光模块），8\*1Gbps Ethernet接口 |
| IO扩展能力 | 双控制器提供≥6个PCIE插槽，用于主机接口扩展 |
| 后端磁盘通道与接口类型 | 配置后端磁盘通道带宽≥192Gbps，端口采用SAS3.0技术，设备可支持NVMe over Fabric，后端支持SAS和MVMe SSD硬盘框和硬盘 |
| 支持硬盘类型 | 支持企业级SAS SSD，非SATA SSD |
| ▲配置硬盘 | 配置≥20个3.84TB企业级SSD硬盘（非SATA接口） |
| 最大硬盘数 | 最大支持磁盘插槽个数≥800 |
| 支持RAID | 支持RAID，提供RAID5、RAID6和容忍三盘失效，提供产品彩页或者官网截图。在同一个RAID组内容忍任意3盘同时失效，数据不丢&不中断业务。重构1TB数据仅需32分钟 |
|  | 存储特性 | 数据保护 | QoS:支持按照LUN、LUN组和主机的方式进行流量控制。提供上限控制和下限保障两种QoS策略，分别都支持从IOPS和带宽两个维度进行配置。同时上限控制策略支持burst配置，下限保障策略支持时延配置。 |
| 1.采用ROW无损快照模式2.支持单LUN ≥6万个快照，系统≥100万个快照；3.系统提供每3秒做一次快照备份，提供可视化管理界面截图，恢复任意时间点快照，其他时间点快照不丢失。4.提供无损快照功能，系统性能不因快照数量增加而下降，同时开启快照功能时阵列时延能够稳定在＜1ms。并提供具备CNAS(中国合格评定国家认可委员会)资质的第三方权威评测机构签字盖章的测试报告 |
| 配置克隆功能，可为快照和源LUN提供一个实体副本。支持克隆立即可用、克隆一致性组、级联克隆、正向和反向同步。分裂后支持实体副本 |
| 配置数据复制功能，把主中心数据复制到另一个数据中心，支持FC和IP两种链路复制，提供官网截图。自定义远程数据异步传输时间间隔，最小支持3S，提供操作页面截图。异步复制支持链路压缩，节省传输带宽，提供操作页面截图 |
| ★远程容灾保护 | 配置存储SAN双活功能1）提供免网关双活架构，实现两套核心存储数据Active-Active双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。2） 一个站点发生故障后，另一个站点可自动快速拉起业务（秒级）；一个站点故障恢复后，双活关系可自动恢复 |
| 异构虚拟化 | 可异构虚拟化1）提供异构虚拟化功能，能够提供异构存储虚拟化整合功能，能接管现网异构存储，无需破坏或者改变现有数据格式，构成异构资源池，进行统一的资源调配和管理。2）异构虚拟化兼容业界主流存储（如EMC、HPE、Hitachi、IBM、Huawei、NetApp、富士通等多个厂家的阵列） |
|  | 多路径软件 | 存储专用多路径软件 | 存储厂商提供专有多路径（非操作系统自带多路径）软件，提供故障切换和负载均衡功能，支持Windows/Linux/AIX/Solaris。提供证明材料截图。 |
|  | 管理维护 | 可维护性 | 支持SSD盘、电源模块、接口不停机热插拔 |
| SSD寿命监控 | 提供SSD寿命监控技术，并在系统中显示每一块SSD硬盘的磨损度以及预估剩余寿命 |
| 智能管理运维 | 支持提前365天容量预测 |
|  | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. PACS存储

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 类别 | 指标项 | 指标要求 |
| 1 | ★架构 | 体系架构 | 实配SAN与NAS统一存储，配置NAS协议（包括NFS和CIFS）、IP SAN和FC SAN协议，不需额外配置NAS网关，存储操作界面同时支持块存储和文件存储功能，提供功能截图证明。 |
| 控制器扩展能力 | 支持控制器扩展，最大支持≥8控 |
| 控制器配置 | 配置双Active-Active控制器；采用2U盘控一体架构，控制器框提供≥24个硬盘槽位 |
| 2 | 配置 | ★控制器处理器 | 采用多核处理器，配置控制器处理器总物理核心数≥16核，提供官网处理器核数截图及链接。 |
| ▲存储缓存容量 | 系统内总一级缓存容量配置≥128GB，且任意控制器一级缓存容量≥64GB（不含任何性能加速模块、FlashCache、PAM卡，SSD Cache、SCM等）控制器缓存均具备断电保护功能，在出现电源故障时，可提供充足的电源，将高速缓存内容转储至非易失性内部存储设备上（非通用服务器架构） |
| 前端主机通道接口 | 可支持配置： 8\*1Gbps Ethernet ＋ 8\*10Gbps Ethernet + 8\*16Gbps FC接口； |
| 后端磁盘通道 | 配置后端磁盘通道带宽≥192Gbps |
| 支持硬盘类型 | 支持SAS SSD、SAS、NLSAS硬盘，并支持混插 |
| ▲配置硬盘 | 配置≥12个8TB 7.2K RPM NL SAS硬盘 |
| 最大硬盘数 | 最大支持磁盘插槽个数≥800 |
| 主机接口热插拔 | 控制器在线运行时，能够对主机接口卡进行热插拔 |
| 支持RAID | 支持RAID 1、RAID3、RAID 10、RAID50、RAID 5、RAID6等可选配置，提供功能截图证明并加盖存储厂商有效印章。支持RAID虚拟化技术，每TB重构时间≤30Min。提供具备CNAS(中国合格评定国家认可委员会)资质的三方权威评测机构签字盖章的测试报告复印件 |
| 3 | SAN软件特性 | 本地数据保护 | 支持数据快照功能，恢复某个时间点的快照，其它时间点快照不丢失 |
| 关键业务保障 | 支持高速缓存分区功能，保障关键业务的隔离和保障，提供具备CNAS(中国合格评定国家认可委员会)资质的三方权威评测机构签字盖章的测试报告复印件 |
| 远程容灾保护 | 支持基于存储产品自身的同步和异步复制软件许可，支持基于FC接口的同步复制功能，达到秒级复制，基于FC链路复制 |
| 支持存储SAN双活功能1）提供双活架构，实现两套核心存储数据Active-Active双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行。2） 双活引擎数据传送必须采用FC协议和链路双活（非IP协议或者IP链路） |
| 4 | NAS软件特性 | NAS功能 | 配置NAS功能，配置NFS、CIFS、NDMP、多租户、目录配额功能；NFS业务支持全局命名空间和日志审计功能； |
| 文件系统全局命名空间 | 多个文件系统能够挂载在根目录，实现全局统一命名空间访问，提供具备CNAS(中国合格评定国家认可委员会)资质的三方权威评测机构签字盖章的测试报告复印件 |
| 重删 | 支持NAS在线重删功能，提升空间的有效利用率 |
| 压缩 | 支持NAS压缩功能，提升空间的有效利用率 |
| NAS一体化备份 | 支持内置备份功能直接将文件系统备份到备份存储，支持配置本地备份策略、异地备份策略；可用本地或者异地备份副本进行恢复 |
| WORM | 支持WORM特性，满足一次写入不可修改和删除，满足关键业务文件信息安全以及法规遵从的要求 |
| NAS双活 | 支持NAS双活功能，单套存储故障，另外一套存储可自动接管FS文件共享特性 |
| 文件缓存分区 | 支持文件系统缓存分区功能，保障关键业务资源使用，为应用系统提供存储服务质量支持，提供软件功能截图 |
| 5 | ★SAN与NAS一体化双活 | SAN与NAS一体化免网关双活 | 支持进行SAN与NAS的一体化免网关双活，任意一套设备宕机均不影响上层业务系统运行（业务不中断）。支持双仲裁服务器配置，支持FC链路复制，SAN双活支持双活流量分担，支持故障自动切换和回切 |
| 6 | 多路径软件 | 存储专用多路径软件 | 存储厂商提供专有多路径（非操作系统自带多路径）软件，提供故障切换和负载均衡功能，支持Windows\Linux。提供国家版权局出具的计算机软件著作权登记证书复印件。提供具备CNAS(中国合格评定国家认可委员会)资质的三方权威评测机构签字盖章的测试报告复印件。 |
| 7 | 资质 | 环保节能 | 产品具有《中国环境标志产品认证证书》或《中国节能产品认证证书》，提供证书复印件或电子件。 |
| 8 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 备份一体机

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 类别 | 指标项 | 指标要求 |
| 1 | 资质 | 著作权证明 | 投标人所投的备份系统软件提供中华人民共和国国家版权局颁发的软件著作权登记证书 |
| 2 | 功能融合 | 备份系统功能 | 一套备份与恢复系统 , 可以支持定时备份保护 |
| 3 | 系统需求 | 系统架构 | 软硬件一体化架构，集备份管理软件，备份服务器和备份存储于一体，无需配置独立备份服务器，无需配置外置备份存储。 |
| ▲实配有效容量（单节点） | 要求硬件实配有效容量≥65TB |
| 备份软件授权 | 备份软件采取后端容量许可方式，容量与硬件实配有效容量相同，不限制备份客户端数量、重删、备份恢复功能等 |
| 4 | ▲备份节点硬件参数（单节点配置以及数量） | 节点数 | 1台 |
| CPU | 处理器要求≥2颗，单颗主频≥3.2GHz，总物理核数≥16 |
| 内存 | 总内存容量最低≥64GB，内存条要求偶数根；要求采用RDIMM或LRDIMM DDR4，频率≥2933内存，支持ECC纠错 |
| 主存储介质 | 要求配置≥12块7200转及以上转速企业级HDD盘，并通过RAID6实现冗余保护，每节点至少配置1块独立的热备盘 |
| 系统盘 | 要求配置2块10000转及以上企业级HDD盘作为独立系统盘，并通过RAID实现镜像冗余保护，单盘容量≥600GB。 |
| 网络接口类型 | 要求实配10Gb以太网光口≥2个，1Gb以太网电口≥2个；要求每个10GbE光口配置多模光模块；可提供扩展接口：10Gb以太网光口支持扩展至6个 |
| 电源配置 | 节点支持220VAC电源模块，提供与部署机房供电匹配的电源模块（其中220VAC要求白金级电源模块）；配置双路（N+N冗余）。 |
| 5 | 标准备份（使用应用接口进行的普通备份特性） | 数据库及应用保护 | 支持对Oracle、SQL Server、DB2、MySQL、SAP HANA、GaussDB、Gbase、PostgreSQL等数据库进行在线备份保护，备份任务配置过程全部图形化操作，无需编写脚本 |
| 支持对Informix、达梦、金仓和神通等数据库进行在线备份保护 |
| 文件系统备份 | 支持Windows、Redhat、SuSE、CentOS、Ubuntu、AIX、Solaris、HPUX、Astralinux、EulerOS、中标麒麟和银河麒麟的文件系统备份恢复 |
| 操作系统备份 | 支持对Windows、Linux操作系统进行在线备份和裸机还原 |
| 卷级备份 | 支持Windows和Linux平台下的文件系统的卷级备份功能，以整卷为单位进行数据备份，提升海量小文件环境下的备份效率 |
| 虚拟化备份 | 支持对VMware、Hyper-V、XenServer、FusionCompute和CAS等主流虚拟化系统的虚拟机备份，无需在需要备份虚拟机内部安装代理 |
| 支持虚拟机自动发现，可自动将资源池或集群中新增的虚拟机纳入到备份作业中，按照既有保护策略进行保护，无需人工干预 |
| 重复数据删除 | 支持源端重删，并行重删；支持全局重删。 |
| 数据安全性 | 支持对备份数据进行加密传输和存储，支持AES256加密算法 |
| 6 | 备份系统管理 | 用户管理 | 支持用户和权限管理，支持管理员/用户/租户权限分离，支持对不同操作用户分配不同的资源、策略和备份管理权限 |
| 统一管理 | 一套备份与恢复系统 , 可以同时支持定时备份、持续备份、持续复制、副本数据管理，实现统一管理 |
| 支持数据备份的集中监控和统一管理，通过单一图形界面实现对备份任务、备份资源、告警信息等的统一管理 |
| 7 | 可靠性 | 备份一体机支持自备份，通过自备份数据集可还原历史配置信息，确保备份数据的可恢复性；自备份数据支持异地远程复制，实现备份一体机系统数据的跨站点数据容灾 |
| 8 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 光纤交换机

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 端口要求 | ▲共24个端口，通过按需增加端口许可证，以12端口的增量增加为12和24个通用端口，本次配置激活24端口，含24个16Gb 多模SFP模块。 |
| 2 | 端口速率 | 2、4、8、16Gbit/sec端口速率自动感应。 |
| 3 | 端口类型 | D\_Port、E\_Port、EX\_Port、F\_Port、M\_Port、U\_Port等。 |
| 4 | 可视化用户界面 | 所有关键部件LED指示灯、基于Web的管理界面和故障定位指示。 |
| 5 | 管理性 | Telnet，HTTP，SNMP v1/v3 (FE MIB，FC Management MIB)；审核，系统日志，变更管理追踪；符合SMI-S标准，SMI-S脚本工具集，管理域。 |
| 6 | 服务 | 提供五年原厂质保 |

1. WEB应用防火墙（WAF）

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | ▲基本要求 | 采用专用硬件架构与专用安全操作系统，基于操作系统内核的完全检测技术；硬件设备可以机架安装，产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能（提供截图证明） |
| 1U,配置≥8个千兆电口，千兆光口≥2个,单电源,应用层吞吐≥2个300Mbps、网络层吞吐≥2个4G、并发连接≥2个100W |
| 2 | ★系统要求 | 为保障系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合TL9000-HSV R6.0/R5.5标准，提供相关证明； |
| 3 | 网络部署 | 无IP纯透明模式串联部署、负载均衡模式部署、反向代理模式部署、旁路监测模式部署 |
| 支持基于域名和IP多种方式提供网站防护。 |
| 支持虚拟线接入，无论任何网络环境可强制数据从一个接口转发到另一个接口（提供截图证明） |
| 支持提取客户端真实IP头；自动尝试匹配X-Forwarded-For, X-Real-IP, Cdn-Src-Ip 用以获取真实客户端IP |
| 支持HTTP/HTTPS站点防护，在代理模式下支持HTTPS流量解析，支持SSL卸载功能。（提供截图证明） |
| 4 | 安全防护 | 支持网络层访问控制，支持基于源IP 地址、目的IP 地址、源端口、目的端口、协议类型及目的区域、地理区域等条件的访问控制。 |
| 支持应用层访问控制功能，针对 HTTP请求字段进行过滤，包括HTTP协议版本，请求方法，Cookie信息等。（提供截图证明） |
| 应能识别和阻断SQL注入攻击,Cookie 注入攻击，命令注入攻击；  |
| 应能识别和阻断跨站请求伪造(CSRF)攻击，支持HTTP token防护和referer匹配防护等多种防护方式。 |
| 支持恶意扫描防护：通过人机识别方式，进行恶意扫描智能检测；支持扫描防护阈值设置和扫描IP的阻断周期设置。（提供截图证明） |
| 支持对网站登录页面提供暴力破解防护功能。 |
| 具备盗链防护功能，防止服务器资源被滥用。 |
| 支持Cookie安全防护，通过对cookie进行加密签名，保障cookie信息安全可信。 |
| 具备WebShell攻击，文件包含漏洞利用、目录遍历等攻击的防护功能  |
| 支持多种爬虫攻击防护：包括但不限于内置爬虫对象库，自定义爬虫对象，导入或者下载后端服务器robots.txt 等方式提供爬虫攻击防护。（提供截图证明） |
| ★支持敏感信息防泄漏功能，可自定义对身份证、信用卡、手机电话号码、座机电话号码、邮箱地址等敏感信息做检查，当检查到此类数据后可通过配置特殊字符\*予以替换隐藏。（提供截图证明） |
| 支持API接口防护：XML基础校验，XML schema校验，WSDL校验。  |
| 支持对文件的上传下载进行控制，包括上传及下载最大文件大小、文件扩展名、MIME类型等进行控制；支持对上传文件内容进行病毒检测的功能。 |
| 支持多重编码检查功能，可对多重的编码均进行安全防御检查，有效防止攻击绕过WAF。（提供截图证明） |
| 支持防护动作自定义，包括告警、拒绝、重定向，错误页面等多种防护动作，同时支持返回错误页面自定义。 |
| 支持对HTTP协议合规性进行验证，提供HTTP协议规范化功能，可自定义最大请求头长度、最大body长度、最大请求行长度、最多cookies个数、最多header头个数等。 |
| 支持自学习建模功能，可以通过学习正常URL参数的长度、参数类型、请求方法等数据特点创建白名单模型，如果参数违反白名单模型则认为是非法流量直接阻断，开启自学习建模功能后可生成自学习网站参数的自学习结果报告。 |
| ★支持虚拟补丁功能，支持导入WAF内置扫描器及appscan、w3af等第三方扫描器的扫描结果生成WAF的防护规则，对此类网站漏洞直接防护。（提供截图证明） |
| 网关型网页防篡改，无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容。 |
| 缓存型网页篡改防护；WAF通过将缓存的网站页面返回给客户端，从而保证客户端无法看到被非法篡改的页面，来做到网页篡改防护。 |
| ★WAF内置WEB漏扫功能，支持深度和快速两种扫描方式对WEB应用漏洞进行扫描检测，支持自定义每日、每周、每月等扫描周期设置，并能够以pdf,html,txt,xml等格式导出web漏洞扫描报告（提供截图证明） |
| 支持WEB缓存,URL重写，HTTP压缩等应用交付功能。 |
| 5 | 数据分析 | 支持对防护的WEB服务器进行健康检查，可以实时监测服务器的活跃状态，并且可定期备份健康记录。 |
| 支持对攻击事件类型，攻击源，URL攻击次数统计，动作统计等WEB安全信息进行可视化展示。 |
| 日志支持以syslog和welf两种格式向远端日志服务器发送日志，日志传输可加密，且管理员可以配置加密密码（提供截图证明）； |
| 针对攻击日志，可对任意一条编辑其行为动作，包括阻断记录日志、阻断不记录日志、继续、警告、临时或永久跳转到某一重定向页面等动作（提供截图证明） |
| 支持日志敏感信息脱敏，记录日志时将敏感数据替换为某个特定字符。 |
| 6 | 系统管理 | 支持邮件告警，告警邮件支持明文传输、支持starttls认证传输、支持ssl的加密传输。 |
| 支持ping、TRACEROUTE、TCP、HTTP、DNS、抓包工具等多种故障诊断方式。 |
| 支持SNMP的V1、V2、V3管理，支持SNMP陷阱主机功能。 |
| 支持账号策略自定义，支持超时重新认证、定义允许最大登录失败次数、密码错误账号锁定时间、最大在线管理员数、对其他非法在线管理员强制下线、防管理员账号暴力破解。 |
| 支持设置向导模式部署，按照设置向导配置，方便安全运维人员快速上线WAF设备。 |
| 支持服务器探测功能，WAF接入后，可自动发现网站服务器的IP及域名信息。 |
| 7 | 高可用性 | 支持双机热备，包括主备、主主负载均衡、连接保护等模式。 |
| 支持两台WAF配置同步，包括全局同步和策略同步两种同步方式。 |
| 支持软件bypass功能，当客户业务流量过载，设备进入紧急模式，保障业务稳定性和连续性（提供截图证明） |
| 支持多服务器的负载均衡模式部署，支持轮叫、加权轮叫、原地址散列、最小连接等多种负载均衡算法。 |
| 8 | ★产品联动 | 支持与本次网络中防火墙联动，提供闭环的Web安全解决方案（提供截图证明） |
| 9 | 资质要求 | 产品具备国家信息安全测评信息技术产品安全测评证书（EAL3+），提供复印件加盖公章具备IPV6金牌证书(专业WAF类)厂商具备中国通信企业协会颁发的通信网络安全服务能力（风险评估二级）评定证书, 提供复印件加盖公章属于国家级应急服务支撑单位；厂商具备中国电子工业标准化技术协会颁发的信息技术服务运行维护标准符合性证书（运行维护），需提供证书复印件设备生产厂家具备信息系统建设及服务能力优秀级（CS4）等级证书；具备能力成熟度CSA CS-CMMI5认证；投标时需提供以上资质证书复印件； |
| 10 | ▲功能测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备工程中无法实现所需的功能，中标后要求投标方提供所投产品对技术指标要求的功能进行逐项测试验证，测试所产生的相关费用由投标方承担，若中标产品未通过测试，将取消中标资格并追究相应责任。 |
| 11 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 堡垒机

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | ▲硬件配置 | 标准1U硬件，含2\*GE电管理口，4\*GE电业务口,硬盘:1T，硬盘不可扩展；1\*RJ45串口，单电源。 |
| 2 | 可管理设备数量 | 授权资产：100个 |
| 3 | 并发性能 | ，最大字符连接100个，最大图型连接20个。 |
| 4 | 系统安装与存储 | 系统须安装在专用的CF卡或固态盘中，审计数据存储在磁盘中，防止操作系统故障导致审计数据丢失。 |
| 5 | 设备部署 | 设备采用旁路部署，不得影响业务环境；须支持HA主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障。 |
| 支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步 |
| 支持集群部署模式，中心采用HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中存储、实时会话集中监控，以满足业务增长需求。 |
| 6 | 用户管理要求 | 用户角色 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理 |
| 用户管理和用户策略 | 支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等 |
| 部门层级管理 | 支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据。 |
| 部门用户管理 | 每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员 |
| 部门资源管理 | 每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略 |
| 部门审计管理 | 每个部门的审计管理员可以管理本部门及下级部门的运维会话日志 |
| 7 | 身份认证要求 | 与第三方认证对接 | 支持与AD、LDAP、RADIUS、吉大正元、北京CA认证系统联动登录堡垒机，[支持自动同步AD/LDAP用户](#_AD/LDAP用户同步) |
| 短信口令认证对接 | 支持与get、post、soap发送方式的http短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动 |
| 手机APP动态口令认证 | 支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令。 |
| 双因子认证 | 堡垒机须内嵌动态令牌和usbkey认证引擎，可同时使用动态令牌和USBkey |
| 多种双因子认证同时使用 | 基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证 |
| 多种认证组合使用 | 支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机 |
| 认证窗口全局设置 | 支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口 |
| 8 | 设备管理要求 | 支持的协议和应用 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具 |
| 主流数据库运维管理 | 支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机 |
| IE代填 | IE代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码 |
| 混合云管理 | 可以通过socks5/http/ssh等代理协议连接管理异地云资源区中私有网络的云主机 |
| 分组管理 | 支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出 |
| 登录模式 | 支持设备帐户和密码的自动登录、手工登录、二次自动登录模式 |
| 自动收集和自动授权 | 支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权 |
| 设备密码管理 | 导出的设备信息文件加密存储，解密时须由2个管理员同时解密才能查看到设备信息文件内容 |
| 9 | 工单流程要求 | 申请工单 | 运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。 |
| 审批工单 | 管理员对运维工单进行审核之后以邮件方式通知给运维人员；如果允许，则运维人员才可访问；否则就无法访问。 |
| 10 | 自动改密要求 | 自动改密 | 支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能 |
| 改密保护机制 | 支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；支持发送方式，包括邮件、FTP、SFTP等 |
| 密码容错机制 | 支持自动密码恢复、手工验证密码、密码强度控制等 |
| 11 | 运维方式要求 | 多种浏览器登录 | Web访问方式：至少支持使用IE、谷歌、火狐三种浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等运维客户端工具 |
| H5运维方式：支持ssh、telnet、rlogin、rdp、vnc协议的H5运维，无需本地运维客户端工具 |
| 数据库运维 | 支持通过堡垒机页面直接调用本地Windows系统里的plsql、sqlplus、toad、sqlwb、ssms、mysql.exe等数据库客户端工具。 |
| 客户端工具登录 | 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力 |
| SFTP/FTP的客户端登录 | 支持使用本地的winscp/flashFXP/SecureFX等客户端工具登录堡垒机访问SFTP/FTP设备 |
| SSH网关代理直连 | 支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备 |
| 数据库代理直连 | 支持在mac电脑里使用navicat工具通过堡垒机登录mysql、oracle等数据库服务器 |
| 批量自动登录字符主机 | 支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量自动登录多台设备 |
| 域用户自动登录主机 | AD/LDAP环境，支持直接使用登录堡垒机的AD/LDAP用户及密码可以直接自动登录到服务器里 |
| 12 | 审计日志要求 | 运维审计日志 | 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。 |
| ★Zmodem传输审计 | 支持保存SSH的sz/rz命令（zmodem）传输的原始文件[并提供第三方权威机构检测报告证明及功能截图](#_SFTP/FTP/zmodem/RDP传输的文件记录) |
| ★SFTP/FTP传输审计 | 支持保存SFTP/FTP传输的原始文件[并提供第三方权威机构检测报告证明及功能截图](#_SFTP/FTP/zmodem/RDP传输的文件记录) |
| RDP粘贴板审计 | 支持保存RDP粘贴板（桌面之间复制-粘贴）传输的原始文件[并提供第三方权威机构检测报告证明及功能截图](#_SFTP/FTP/zmodem/RDP传输的文件记录) |
| ★RDP磁盘映射审计 | 支持保存RDP磁盘映射传输的原始文件[提供第三方权威机构检测报告证明及功能截图](#_SFTP/FTP/zmodem/RDP传输的文件记录) |
| RDP文字记录 | 支持对RDP屏幕文字内容、标题窗口、键盘输入的记录和搜索定位 |
| SQL记录 | 支持审计主流数据库（如DB2、oracle、mysql、sql server）运维中的SQL语句，可进行关键信息定位查询 |
| 全文检索 | 支持全局搜索审计日志，无需区分图形/字符/文件/应用类型，只需通过关键信息直接搜索定位 |
| 日志数据归档 | 审计数据支持通过SFTP/FTP方式自动归档，并在页面中可以查询哪些数据是否归档，可以设置归档成功之后自动删除数据，归档后的数据可以用专用播放器离线查看 |
| 13 | 安全策略要求 | 运维规则策略 | 支持通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。 |
| 二次审批 | 对重要设备启用登录审核功能，运维人员须向管理员申请登录，管理员允许之后才可登录；否则无法登录 |
| 命令审批 | 支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功 |
| 自动运维任务 | 支持自动推送命令任务，如可自动备份交换机/路由器的配置信息、可自动执行周期任务；并将结果以邮件/FTP/SFTP的方式发送给相关管理员 |
| 运维空闲时间限制 | 支持运维空闲会话时间全局设置限制功能 |
| 14 | 报表统计要求 | 运维报表格式 | 内置丰富的报表统计模板，可点击柱状图、饼状图或曲线图进行数据钻取分析，且支持PDF、doc、html格式导出 |
| 运维报表内容 | 内置根据运维人员和组生成各种维度的分析报表，维度包含总为运维次数、时长、活动时长、会话起止时间、会话大小、命令数、上传下载文件数，分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供非常有价值有意义的报表 |
| 自动发送报表 | 支持运维报表自动定期发送，提供一键导出符合等级保护、SOX法案要求的综合分析报告 |
| 15 | 系统管理要求 | 系统自审 | 支持自身审计，包括但不限于：系统状态检测、登录日志、用户配置日志、设备配置日志、授权配置日志、策略配置日志、运维访问日志、系统配置日志等 |
| 系统日志报表 | 支持系统日志报表统计功能，包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表 |
| 告警输出 | 支持邮件/syslog方式输出告警日志 |
| SNMP输出 | 支持SNMP方式输出系统信息 |
| 排错功能 | 提供排错工具：ping、TCP端口检测、UDP端口检测、路由跟踪等 |
| API接口 | 需提供用户、资产、授权的增删改查等API接口，允许第三方平台调用堡垒机的API接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量 |
| 与同品牌数据库审计联动 | 支持和同品牌数据库审计系统进行联动，将通过SSH/RDP等加密方式操作数据库的行为整合到数据库审计中，实现数据库行为的统一集中查询、展示、审计分析等 |
| 与同品牌SOC联动 | 支持和同品牌的SOC系统进行联动，对绕过堡垒机而登录主机的行为，SOC进行实时告警，并且与SOC进行日志关联性分析 |
| 16 | 产品资质要求 | [产品需获得公安部产品销售许可证](#_销售许可证) |
| 17 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 内网专线防火墙

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | ▲基本要求 | 所投产品必须为下一代防火墙，非UTM或其他产品，产品采用X86多核及自主知识产权的多核并行安全操作系统构成； |
| 1U, 配置≥6个千兆电口，SFP插槽≥8个,冗余电源,防火墙吞吐≥8G，并发连接≥150万，每秒新建连接≥3万，IPSEC VPN吞吐≥80M，SSL VPN吞吐≥220M |
| 2 | ★系统架构 | 为保障系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合TL9000-HSV R6.0/5.5标准（提供相关证明）； |
| 要求支持防火墙芯片硬件加速技术，实现硬件资源充分利用，保障设备处理效率，提供第三方权威证明材料 |
| 3 | 网络接入 | 支持路由、交换、虚拟线、Listening、混合工作模式； |
| 支持根据入接口、源/目的IP地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由； |
| 支持链路聚合，可根据源/目的mac、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法；（提供截图证明） |
| 支持DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡；（提供截图证明） |
| 支持SIP协议的媒体业务接入，实现内外网媒体系统之间上联和下联安全防护。 |
| 4 | 安全控制 | 内置P2P应用、加密应用、数据库应用、工控物联网协议等应用特征库；支持应用特征库在线或本地更新，支持自定义应用特征； |
| 提供策略命中、冗余、冲突、包含检查及策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度查询；（提供截图证明） |
| 内置文件过滤引擎，支持HTTP/FTP/SMTP/POP3等标准协议进行检测，识别可执行文件、office文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过50种文档类型的文件过滤； |
| ★支持一体化安全策略配置，通过一条策略实现五元组、源MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、WAF、URL过滤、邮件安全、数据过滤、文件过滤、审计、APT等功能配置，简化用户管理；（提供截图证明） |
| 内置防代理功能，阻断网络用户通过代理主机进行攻击、共享上网等行为； |
| 内置内容过滤功能，可对FTP上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤；（提供截图证明） |
| 支持将五元组、源MAC、地址范围、应用、用户等加入静态黑名单，可与URL过滤、病毒过滤、防代理功能进行联动实现动态黑名单封锁，支持静态和动态黑名单命中统计和监控；  |
| 支持连接控制和监控，可对源/目的地理对象、应用制定连接限制策略，可展示被拦截的IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息；  |
| 5 | 安全防护 | ★内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供截图证明） |
| 支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护； |
| 支持NTP流量检测清洗，能对NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击进行检测并提供基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；（提供截图证明） |
| 内置邮件安全防护功能，可进行匿名发件人、收发件人同名、非标客户端、收/发件人频率、收/发件IP频率、邮件长度、附件名称、附件数量检测，支持黑、白名单检测； |
| 支持基于UDP协议的检测清洗，包括对源、目的限速，对UDP最大及最小报文限制；支持UDP关联认证，对源地址进行合法性认证； |
| 支持DNS FLOOD防护，能对DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒、DNS格式等攻击提供DNS REPLY源认证、源限速、目的限速、域名限速等综合防护手段；（提供截图证明） |
| 5 | 系统管理 | 支持主、备双系统以及多个系统版本文件并存，系统版本数量不少于5个； |
| ★支持多个配置文件并存，配置文件备份能力不少于4个（提供截图证明）；配置文件支持选择部分配置和全部配置导入导出； |
| 6 | 数据中心 | 支持独立审计策略，可对URL地址、网页标题、网页内容、邮件行为、邮件内容、FTP上传/下载行为及文件内容进行审计； |
| 提供完善的审计数据查询功能，可对用户访问网站、邮件收发、论坛微博、FTP、TELNET等上网行为以及用户上网流量时长等内容进行查询；  |
| 支持日志本地存储，可对不同类型日志设置存储空间，支持日志外发至多个服务器，可设置日志传输协议、时间类型、日志语言、是否合并及加密传输等参数；  |
| 7 | 显示监控 | 支持对设备CPU、内存、磁盘、整机流量、新建、并发进行统计，展示设备CPU、内存、硬盘实时利用率及其历史走势图； |
| 支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；（提供截图证明） |
| 8 | ★产品资质 | 投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，连续5年市场占有率排名不应低于前3名。须提供知名第三方机构IDC出具的市场占有率排名有效证明材料。具备产品成熟度CSA CS-CMMI5认证；投标时需提供以上资质证书复印件； |
| 9 | 厂商资质 | 厂家具备通信网络安全服务能力风险评估二级；厂家具备信息系统建设及服务能力优秀级（CS4）等级证书； 厂商具备中国电子工业标准化技术协会颁发的信息技术服务运行维护标准符合性证书（运行维护）投标时需提供以上资质证书复印件； |
| 10 | ▲测试验证 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备工程中无法实现所需的功能，中标后要求投标方提供所投产品对技术指标要求的功能进行逐项测试验证，测试所产生的相关费用由投标方承担，若中标产品未通过测试，将取消中标资格并追究相应责任。 |
| 11 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 网闸

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | ▲硬件要求 | 2U,内外端机双侧液晶屏；内端机≥6个10/100/1000Base-T接口，2个SFP插槽，1个扩展槽位，含1个MGMT口；外端机≥6个10/100/1000Base-T接口，2个SFP插槽，1个扩展槽位，含1个HA口；,冗余电源,网络吞吐量≥1Gbps；并发连接数≥12万；内外端机各1TB硬盘。 |
| 2 | 系统架构 | 2+1”系统结构，内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通。内外端机之间采用专用硬件和专用协议进行连接，不可编程。 |
| 3 | ★产品形态 | 软硬件一化设备；为保障系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合TL9000-HSV R6.0/5.5标准，软件通过CIMM5成熟认证，提供相关证明； |
| 4 | 硬件架构 | 硬件架构由内端机、外端机、专有隔离硬件三部分组成。内端机和外端机各自具有独立主板、独立总线、独立的存储和运算单元；内端机和外端机之间非网线、USB线、SCSI线等线缆直连，基于光隔离技术专有硬件进行隔离和数据交换。 |
| 5 | 管理架构 | 管理控制层和业务数据层分离，管理系统部署于内端机上， 只能通过内端机上的管理口对网闸进行配置，不允许外端机存在任何形式的管理接口。可避免黑客从外部网络入侵，导致隔离网闸被黑客完全控制的现象。(提供产品图片) |
| 6 | 安全浏览功能 | ★支持访问控制日志记录和告警功能；支持最大活动会话数的控制和统计；支持IPV6扩展头的安全设置。（请提供相关截图） |
| 支持基于单一域名的黑白名单访问控制，支持基于URL分类地址库的访问控制，支持允许、阻断、告警三种处理方式 |
| 支持http消息头、消息体，上下行方向，命令及关键字的管控，支持允许、阻断、告警三种处理方式。（请提供相关截图） |
| 内置HTTP安全模块，支持URL过滤引擎、内容过滤引擎、文件过滤引擎、病毒过滤引擎、网页过滤引擎安全防护及单独启停控制。 |
| 7 | 文件传输功能 | 支持访问控制日志记录和告警功能，支持最大活动会话数的控制和统计；支持IPV6扩展头的安全设置。 |
| 支持FTP协议内部命令及数据层内容过滤，支持允许、阻断、告警三种处理方式。 |
| 内置FTP安全模块，支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制。（请提供相关截图） |
| 8 | 数据库访问功能 | 支持访问控制日志记录和告警功能；支持最大活动会话数的控制和统计；支持长连接设置；支持IPV6扩展头的安全设置； |
| 内置数据库安全模块，支持内容过滤引擎，能够对数据库用户名、命令、关键字等内容进行管控，支持允许、阻断、告警三种处理方式。 |
| 9 | 安全邮件功能 | 内置邮件安全模块，支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制。（请提供相关截图） |
| 10 | 安全VOIP功能 | 支持访问控制日志记录和告警功能，支持最大活动会话数的控制和统计；支持IPV6扩展头的安全设置； |
| 内置VOIP安全模块，内置VOIP安全引擎，支持主被叫用户黑名单的控制。（请提供相关截图） |
| 11 | 自定义访问功能 | 支持访问控制日志记录和告警功能；支持最大活动会话数的控制和统计；支持IPV6扩展头的安全设置。（请提供相关截图） |
| 12 | 支持扩展文件同步功能模块 | 支持源文件处理策略，包括保留、删除、转存三种处理方式。支持同步删除、文件续传、子目录同步、日志记录开关控制；支持单一任务的线程数和缓冲时间设置，可手动设置同步任务的线程数； |
| 支持基于文件大小和文件修改时间的同步策略，可手动指定上下限阈值。 |
| ★支持文件同步信息统计，包括每个任务的开始时间、同步数据量、同步成功数、同步失败数，并能够以图表的方式进行实时可视化展现。（请提供相关截图） |
| 13 | 支持扩展数据库同步功能模块 | 支持自动读取数据库表名和字段名，无需手动录入表名和字段名，降低配置复杂度。 |
| ★支持网闸同侧数据库之间的数据同步，网闸可旁路部署实现数据库同步。（请提供相关截图） |
| 快速配置支持全库表同步，可直接映射两个独立数据库进行同步，支持每策略映射表数量控制，支持每策略映射同步方向控制。 |
| 支持数据库同步冲突策略处理，包括覆盖、忽略、以源为准、以目的为准等处理方式。 |
| 支持数据库同步信息统计，包括每个任务的开始时间、同步成功数、同步失败数，同步忽略数，并能够以图表的方式进行实时可视化展现。 |
| 14 | 入侵防御功能 | 支持HTTP攻击类，RPC攻击类，WEBCGI攻击类，拒绝服务类、木马类、蠕虫类等11大类不少于4000条的攻击规则知识库。（请提供相关截图） |
| 15 | DDOS防护功能 | 支持DOS攻击防御，支持端口扫描防御、IP扫描防御、支持IP\TCP\UDP源限速和目的限速，可手动设置相关阈值。 |
| 16 | 安全防护功能 | ★提供连接保护功能，支持基于源和目的IP地址的并发连接数和新建连接数控制，并可以手动设置相关阈值，超过阈值后可选限制和警告两种处理方式。（请提供相关截图） |
| 提供IPV4\IPV6双栈IP+MAC绑定功能，支持基于物理接口和IP网段的IP+MAC主动探测，支持IP、MAC信息查询功能。（请提供相关截图） |
| 17 | 用户认证功能 | 提供本地认证功能和外部认证功能，外部认证支持Radius、Ldap、Tacacs等类型的认证服务器。 |
| 支持认证页面的门户配置，支持认证用户的界面保活，可手动设置保活时间。 |
| 18 | 网络管理功能 | 支持IPV4/IPV6双栈基础路由配置和邻居学习。 |
| 提供服务器负载均衡功能，支持轮询、加权轮询、最少连接、加权最少连接等负载均衡算法。（请提供相关截图） |
| 19 | 设备监控功能 | 提供应用流量监控，以图表形式实时展现内外端机TOP10应用流量排名，包括上下行流量、总流量和流速信息。 |
| 提供威胁统计监控，以图表形式实时展现内外端机TOP20的病毒防御威胁事件统计排名。 |
| 提供在线用户监控，可实时展现内外端机在线用户名称、IP地址、认证服务器名称、客户端类型和在线时间信息，并可根据管理需要手动强制指定用户下线。（请提供相关截图） |
| 20 | 系统管理功能 | 管理端通过独立的管理口与网闸内端机相连，策略统一从内端机下发，不允许采用外端机上的任何网络接口进行管理。 |
| 提供统一的https管理界面，支持ssh和telnet远程管理，支持配置文件的加密导入导出。 |
| 提供ping、traceroute、tcp、udp、http、dns等诊断诊断测试工具，支持设备健康记录和调试信息的导入导出。 |
| 提供告警功能，支持邮件、声音、控制台、SNMP等多种告警方式。 |
| 21 | 资质要求 | 公安部GB/T28181-2016《公共安全视频监控联网系统信息传输、交换、控制技术要求》检测报告厂商具备中国信息安全评测中心颁发的信息安全服务（风险评估类二级）资质证书；厂商具备中国电子工业标准化技术协会颁发的信息技术服务运行维护标准符合性证书（运行维护），需提供证书复印件设备生产厂家具备信息系统建设及服务能力优秀级（CS4）等级证书；具备能力成熟度CSA CS-CMMI5认证；投标时需提供以上资质证书复印件； |
| 22 | ▲功能测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备工程中无法实现所需的功能，中标后要求投标方提供所投产品对技术指标要求的功能进行逐项测试验证，测试所产生的相关费用由投标方承担，若中标产品未通过测试，将取消中标资格并追究相应责任。 |
| 23 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 态势感知

|  |  |  |
| --- | --- | --- |
| **序号**  | **指标项** | **指标要求** |
| 1 | ▲硬件规格 | 硬件外形：软硬一体化2U标准机架式设备； 电源：1+1冗余电源 CPU：4核4线程\*1 内存：16G 硬盘容量：2T\*1 接口数量：标配6个； 接口类型：千兆RJ45网口\*2(管理口\*2)、千兆RJ45网口\*4接口扩展：千兆SFP光口\*4  |
| 2 | 高可用性 | 部署方式 | 旁路镜像模式部署，不影响服务器处理性能和网络架构； |
| 分布式部署 | 支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和IP，管理中心可实现告警统一管理；可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数； |
| 3 | 性能规格 | 吞吐率：网络层：2Gbps应用层：1GbpsWEB检测：HTTP最大并发数7万/秒邮件检测：邮件处理数: 150万封/24小时文件检测：5万个/24小时支持管理节点10个 |
| 4 | 攻击检测 | 全流量检测 | 支持全流量检测，可根据需求打开或关闭全流量检测功能 |
| 审计协议 | 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle、HTTPS、SMTPS、POP3S、IMAPS等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号；支持LDAP登录行为识别；支持VXLAN镜像流量解析检测 |
| 检测风险类别 | 支持检测WEB攻击、异常访问、恶意文件攻击、远程控制、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、WEB行为分析、隐蔽信道通信、暴力破解（包括SSH、TELNET、RDP、FTP暴力破解）、挖矿等风险 |
| 告警黑白名单过滤 | 支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB风险特征白名单进行设置 |
| 私网IP地理位置定义 | 支持对私网地址IP地理位置信息添加，在产生告警时，定义IP可正常显示所属地理位置信息 |
| 弱口令风险检测 | 支持对Telnet、FTP、POP3、SMTP、IMAP等协议进行弱口令检测 |
| 告警详细展现 | 可支持详细展现告警级别、时间、威胁名称、状态、客户端IP、客户端IP所在地理位置、服务端IP、服务端IP所在地理位置、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie、请求参数、响应码、返回长度等信息 |
| 主机威胁分析 | 可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等 |
| 可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析 |
| 可通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示 |
| 木马回连分析 | 可自动学习网络流量中包含的各种可疑C&C IP/URL，包含各种可能对内网存在影响的IP和域名 |
| 快速识别网络中存在的恶意回连行为，包含回连主机IP、服务器IP、时间、行为等 |
| 对基于木马回连的非法数据传输等行为进行取证分析，包括回连主机IP、服务器IP、传输数据大小、协议类型等 |
| 攻击地图展示 | 可通过攻击源和目的的地理位置信息，以世界地图和中国地图的形式展示，并实现世界地图和中国地图自动切换直观展示攻击路径 |
| 5 | WEB攻击检测 | 协议解析 | 支持 HTTP、HTTPS（需要导入服务器私钥证书）协议解析，检测WEB攻击 |
| 双向审计 | 支持双向审计，对请求和响应都进行审计 |
| 攻击检测 | 支持SQL注入、命令注入、跨站脚本、代码注入、协议错误攻击检测 |
| WEBSHELL检测 | 支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功 |
| 自定义WEB审计规则 | 支持根据来源IP、MAC、HTTP请求方法、URL、请求头、请求参数、响应码等内容设置审计规则高、中、低等风险等级 |
| 白名单功能 | 支持WEB特征攻击风险白名单设备，可基于类别、规则、IP灵活配置 |
| 动态分析 | 自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等。 |
| 场景化分析 | 支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT攻击等事件进行预警。 |
| DNS协议分析 | 具备DNS协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连C&C域名、DNS返回详情、恶意主机明细等行为。 |
| 与WAF联动 | 支持将分析到的WEBSHELL攻击、木马回连和恶意攻击行为同步到WAF，实现APT深度威胁分析与WAF联动阻断 |
| 6 | Mail攻击检测 | 协议解析 | 支持解析webmail、SMTP、POP3、IMAP、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）类型报文 |
| Webmail攻击检测 | 支持基于webmail攻击类型检测，包括sql注入、跨站、命令注入等攻击检测 |
| ★社工类攻击检测 | 对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接（提供截图证明，并加盖公章） |
| 恶意附件检测 | 支持邮件恶意附件行为检测 |
| 7 | 文件攻击检测 | 解析协议 | 支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输文件检测 |
| 文件类型 | 支持doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html，js等多种文件解析 |
| 自定义文件类型 | 可添加或删除指定分离的文件类型，并可选择适用的协议类型（HTTP可进一步按GET、POST来配置） |
| 特征检测 | 对文件进行特征匹配，利用已知的特征库发现恶意的可执行文件及非可执行文件。 |
| ★Shellcode检测 | 通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击（提供截图证明，并加盖公章） |
| 动态沙箱检测 | 对存在问题的文件输出完整的二进制动态分析报告动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险对文件关键行为进行截图可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容可展示ROP行为检测可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、进程运行的函数、返回结果、返回值等信息可显示文件运行过程中企图访问的IP、域名，以及域名及对应的IP |
| 子文件扫描 | 对文件内部嵌入的子文件可进行二次扫描，分析安全性 |
| 攻击样本提取 | 可以提取出攻击的完整样本文件，并提供对该文件下载的能力 |
| 文件威胁指数 | 可展示威胁程度最高的文件样本MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容 |
| 根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机host和完整沙箱分析报告 |
| 根据云端威胁情报展示云端是否确认、传播协议类型、传播次数、云端确认结果等 |
| 8 | 失陷主机检测 | 远程控制检测 | 支持根据威胁情报、DGA域名请求、IDS规则、用户配置数据，发现被远程控制的内部主机 |
| DGA域名请求检测 | 具备DNS协议解析功能，发现发起DGA域名请求的失陷主机 |
| 挖矿行为检测 | 可发现利用失陷主机挖矿的行为 |
| 9 | 威胁情报与APT云端 | 本地威胁情报 | 设备集成离线的高可用威胁情报库 ，支持离线环境下，根据威胁情报进行检测，增量威胁情报随策略升级包升级 |
| 云端威胁情报 | 支持自动从APT云端获取最新威胁情报 |
| 协同防御 | 支持将本地恶意文件攻击的病毒类型等信息上传到APT云端，提升协同防御能力 |
| 策略自动更新 | 支持自动从APT云端更新策略 |
| 紧急事件上传 | 支持紧急事件上传云端，帮助客户关注紧急事件 |
| 10 | 抓包检测功能 | 抓包任务 | 同时支持至少16个抓包任务抓包，每个抓包任务可配置抓包规则，按照IP、端口、协议等信息进行抓包，将抓取的原始流量包保存于本地以供后续分析和取证使用，每抓包任务最大抓包20MB |
| 11 | 管理功能 | 三权分立用户管理 | 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持自定义管理用户权限和角色 |
| 风险处理 | 支持根据需要对风险状态进行选择处理中、处理完成、延迟处理、拒绝处理等 |
| 一键登录排错 | 支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。 |
| 设备状态监控 | 支持对设备的CPU、内存等状态进行监控，并在设备界面中进行展示  |
| 知识库 | 根据不同的风险信息，提供风险分析和处置建议知识库； |
| 12 | 日志报表 | 告警与报表 | 告警可详细展示风险级别、发生时间、告警名称、客户端IP、服务器IP、报文内容（URL、请求头、请求参数、请求内容） |
| 可根据需要针对单个告警添加白名单 |
| 支持kafka、短信、邮件、syslog、snmp、ftp等告警方式 |
| 支持对kafka、syslog发送的风险信息进行AES加密传输 |
| 支持同时发送多人、单条发送、发送统计等高级告警功能； |
| 报表能够支持WORD、PDF等格式导出； |
| 日志数据管理 | 审计数据保留策略应至少满足天数和百分比两个控制参数，支持web界面可配置，且恢复数据不影响正常的审计功能。对审计日志可自动备份并加密，必须导入设备才能进行恢复查看，并可自动释放磁盘空间。 |
| 13 | 售后服务支持 | 售后服务 | 提供5年免费升级与维护服务 |
| 提供24小时支持热线； |
| 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 数据脱敏

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 基本要求 | 易用性 | 系统基于B/S架构web管理模式，提供中文操作界面，无需安装任何客户端或者代理。支持Linux、Windows、UNIX等操作系统。 |
| 稳定性 | 脱敏系统平稳运行，满足高峰交易处理的需要，使用过程中不出现crash，进行脱敏操作的过程中不需要频繁重启后台服务，脱敏操作对数据库(源库和目标库)影响小。 |
| 2 | 配置要求 | 硬件规格 | 2U机架式设备：双电源、6个电口、1×扩展槽位、16G内存、128G SSD、2T存储空间。含脱敏数据源容量授权1T,5年原厂质保服务 |
| 3 | 功能要求 | 数据源和目标 | 系统支持丰富的数据源和目标，数据源、目标配置通过系统界面实现（投标时提供功能截图）：1、支持Oracle、DB2(包含AS400/UDB)、Sql Server、Sybase、Mysql、PostgreSQL、MariaDB、informix、人大金仓、达梦、南大通用（gbase 8t/8s）、cache关系型数据库。2、支持Teradata、Gbase 8a、TiDB、GaussDB、SAP HANA等数据仓库脱敏。3、支持hive、impala、Hbase、MongoDB、MaxCompute、TDH、ADS、RDS、巨杉等大数据平台脱敏。4、支持直接读取txt、csv、excel、xml、json等文件、DICOM等医疗影像文件、oracle dump（exp/expdp）、mysql dump（sql文件）等各类文件进行脱敏。 |
| 脱敏方式 | 数据脱敏过程不落地，无需额外存储中间数据。 |
| 支持源库到目标库脱敏（包含支持同库脱敏）、数据库到文件脱敏、文件到文件脱敏（包括FTP和SFTP方式）、文件到数据库脱敏。 |
| 支持主流关系型数据库（Oracle、DB2、SQL Server、Mysql）之间的异构脱敏、关系型数据库（Oracle、DB2、SQL Server、Mysql）与大数据平台之间的异构脱敏。（投标时提供功能截图） |
| ★支持多种增量脱敏方式，包含但不限于通过时间戳、主键或自定义列的方式进行增量脱敏，通过cdc或ogg等日志增量模式。（投标时提供功能截图） |
| 支持Oracle等数据库在脱敏时自定义选择目标表空间。 |
| 支持关系型数据库，文件类，大数据平台，数仓等多种数据源的增量脱敏。 |
| 敏感信息发现 | ★支持通过抽样的方式进行敏感数据发现，可自定义发现规则、抽样比例和匹配率，系统内置的发现规则包括：中文姓名、英文姓名、姓名拼音、韩文姓名、电话号码、邮箱、邮编、金额、日期、企业营业执照、组织机构代码证、银行卡号、军官证、港澳通行证、往来台湾通行证、护照、税务登记证、身份证、组织机构名称、地址、IP地址、社会统一信用代码、开户许可证、医疗机构登记号、医师资格证书、医师职业证书、证券代码、证券名称、基金名称、基金代码、车牌号码、JSON等。（投标时提供功能截图） |
| 支持自动检测源数据库DDL的变动，识别增量数据的敏感信息。 |
| 支持混合类型的敏感数据发现：一个字段多种敏感类型、一个数据单元内多种敏感类型。 |
| 支持针对单个字段手动设置敏感类型。 |
| ★支持电子病历等拥有一定规律的半结构化文本敏感发现，自动发现文本中的相关敏感信息。（投标时提供功能截图） |
| 脱敏规则管理 | 可自定义增加脱敏规则，提供SHA1加密、MD5加密、AES加密、RSA加密、随机映射、固定映射、替换、截断、截取，以及保留、取整、范围内浮动、比例内浮动等各种脱敏算法；支持分段配置不同的脱敏规则。（投标时提供功能截图） |
| 支持数据脱敏后保持原有数据特征、关联性、一致性（同一库、不同库）。 |
| 支持依赖脱敏，可根据依赖字段的值对数据进行不同类型的脱敏处理。 |
| 支持计算脱敏，数据脱敏后保留计算关系，如数据的分组求和、依赖计算等。 |
| 支持组合脱敏，选择多个敏感类型形成组合，组合内所有敏感类型都存在时才进行脱敏。 |
| 支持脱敏策略配置功能，组合多个敏感类型和对应的脱敏规则，形成脱敏策略。 |
| 支持对电子病历等拥有一定规律的半结构化文本中的敏感信息，进行脱敏处理。 |
| 支持配置脏数据处理规则，原值输出或者使用通用脱敏。 |
| 脱敏管理 | 系统自动检测源数据库DDL变动，自动同步变化的对象。 |
| 核心敏感数据可通过黑名单过滤，不脱敏或不迁移到目标端，提供独立管理页面。 |
| 支持对已发现敏感类型的数据重复、合并、筛选使用，无需进行敏感数据的再次发现。 |
| ★支持表(包含分区表、簇表、索引组织表、队列表、压缩表、嵌套表)、主键、外键、索引（包含分区索引、位图索引、函数索引、压缩索引）、约束、视图、同义词、序列、队列、DBlink、自定义类型、存储过程、函数、触发器、包等数据库对象脱敏后在目标库中自动创建。（投标时提供功能截图） |
| 支持在脱敏前对脱敏结果进行预览，确定脱敏效果。 |
| 支持创建测试数据子集，对包含的敏感信息进行脱敏，可在界面创建子集抽取规则（如：百分比、记录数以及根据相关条件设置）。 |
| API接口调用 | 支持第三方系统调用API脱敏接口对JSON、XML文本进行敏感数据脱敏。 |
| 支持作业调度API，可通过API对于作业进行启动、暂停、终止操作，可通过该API查看作业当前的运行状态、处理的数据量、同步对象数量、处理进度、处理耗时等。（投标时提供功能截图） |
| 作业管理 | 1. 支持脱敏作业定时调度，可在指定时间自动运行；
2. 支持作业分段运行管理，可配置运行时段和暂停时段。
 |
| 脱敏作业运行状态可视化展现，包含脱敏作业状态、效率（如：10000行/s）、进度条、当前脱敏操作等监控指标； |
| 有精细脱敏作业阶段，如对于库到库的脱敏至少包含预处理、数据库对象同步、脱敏数据同步、索引创建、约束启用等不同阶段。 |
| 支持对已设置为数据源的库信息做强阻断性保护，防止操作不当导致的源数据被删除。 |
| 授权和审核 | 完善的授权体系，可对数据源中的库、表或者脱敏作业，进行单独或批量授权给单用户或用户组。 |
| 拥有脱敏作业审核流功能，针对单独脱敏作业，可配置专人审核后方可运行。（投标时提供功能截图） |
| 邮件告警 | 支持邮件告警功能，当作业运行结束、暂停、终止、异常停止、异常终止等作业状态发生变化的时候发送邮件。 |
| 4 | 安全性要求 | 账户安全 | 系统支持AD域验证登录。 |
| 脱敏系统具有管理员、安全员、审计员，实现三权分立。 |
| 脱敏系统操作日志全程记录，并可以将日志同步第三方。 |
| 支持脱敏系统自身定时或者手动备份，支持从备份中恢复脱敏系统。 |
| 具备防暴力破解机制，连续登录不正确次数达到阈值后锁定10分钟。 |
| 5 | 资质要求 | 产品资质要求 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| 具备CCRC颁发的《IT产品信息安全认证证书》 |
| 6 | 功能验证 | 功能验证 | 中标后，招标人有权要求中标方提供产品进行相关功能验证，如存在虚假应标行为，将废除中标资格，并依法追究相关法律责任。 |
| 7 | 服务 | 售后服务能力 | 要求原厂实施项目团队成员具备良好的数据库技术支持能力以保障本系统的顺利运行，项目团队成员具体要求如下：1、项目经理同时具备PMP认证证书和OCM认证证书；2、实施工程师同时具有OCP认证证书和CISP认证证书。 |
| 服务 | 五年原厂质保 |

1. 上网行为管理

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | ▲硬件要求 | 1U,千兆电口≥6个，支持1对Bypass，SFP插槽≥2个，2个可插拔扩展槽,单电源,扩展槽位≥2个：适配带宽≥400M，推荐用户数≥3000 |
| 2 | 部署模式 | 支持路由模式，旁路模式、网桥模式、混合模式部署； |
| 3 | 即插即用 | 支持即插即用功能。不管电脑的IP如何配置，开启即插即用功能后，只要插上网线，即可上网（提供截图证明） |
| 4 | 系统架构 | 为保障系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合TL9000-HSV R5.0/5.0标准，提供相关证明； |
| 5 | 安全策略 | 支持基于策略方向、源地址、目的地址、服务、生效时间的安全策略。（提供截图证明） |
| 6 | ★系统存储空间 | 系统CF卡≥4G，设备本身的操作系统单独存放在CF中，要与日志存储分开。（提供厂家相关证明） |
| 7 | 链路聚合 | 支持将多个以太网物理端口捆绑成一条逻辑端口（即将多个端口捆绑成一个逻辑的端口以增加带宽，同时增加链路备份）支持基于轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等多种负载方式。（提供截图证明） |
| 8 | 对外攻击防护 | 支持基于源地址（允许任意地址、允许指定IP其他阻断此两种源地址）过滤的方式，通过部署环境的不同（三层或者二层），设置单日的端口TCP最大连接数、最大攻击包次数、封锁攻击时间等。另外支持设置排除地址。 |
| 9 | 管理认证 | 支持管理员通过Radius认证后才能登录设备。（提供截图证明） |
| 10 | APP集中监控功能 | 支持行为管理设备接入集中管控平台，并通过APP管理集中管理平台并查各个局点的ACM的状态和告警信息 |
| 11 | ★加速老化 | 支持对TCP、UDP、ICMP、TCP SYN超时时间，无回应UDP超时时间设置，并能支持按照新建会话与总会话比例设置老化开始或者结束。（提供截图证明） |
| 12 | 用户有效期设置 | 支持临时账户、绑定账户、认证账户等多种用户身份的有效期设置，支持过期冻结、支持无流量自动下线。 |
| 13 | 用户密码策略 | 支持管理员自定义密码复杂度，多种组合方式，另外支持密码有效期。 |
| 14 | NetbIOS 协议扫描 | 可通过 NetbIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理。 |
| 15 | 跨三层mac识别 | 支持通过snmp服务读取下层三层设备的arp表象获取客户真实的mac地址。 |
| 16 | 临时账号设置 | 支持临时账号自动申请功能，方便外来的临时用户使用。支持自动审核和管理员手动审核的核定方法将临时帐户加入到组织结构中。支持网页发送和邮件方式通知临时用户账号和密码（提供截图证明） |
| 17 | 邮件过滤 | 支持基于支持邮件的“发件人/主题关键字/内容关键字/附件类型”过滤（POP3/SMTP/Web Mail），支持ssl加密邮件内容和标题的识别和过滤。 |
| 18 | 告警 | 设备内存、cpu、会话、接口速率支持告警设置；支持时间告警，支持黑名单告警；支持违规网站、违规搜索、违规帖子、违规上传、违规邮件、还有潜在威胁的告警行为；（提供截图证明）告警策略要支持syslog、短信、邮件、日志记录，以及任意的方式组合。（提供截图证明） |
| 19 | 白名单 | 支持url白名单，添加到白名单的url不受策略控制和审计。支持ip白名单，添加到白名单的ip不受策略控制和审计。 |
| 20 | 定义URL | 网关支持管理者自定义新的URL地址和URL分类； |
| 21 | 关键字过滤 | 关键字组支持通配符配置，支持论坛、微博发帖关键字过滤，支持搜索引擎关键字过滤，支持邮件内容、正文标题、附件内容的关键字过滤，支持包含制定关键字的页面过滤。 |
| 22 | 基于连接数限制 | 支持每个用户的源，目的活跃连接数控制，避免网络滥用 |
| 23 | 应用限额 | 支持基于每天的时长、流量、服务、每天登陆次数和单词在线时长来显示用户使用网络，达到限额限制后会提示相关用户在应用限额限制内。 |
| 24 | 可与同公司的终端检测防御系统实现联动 | 支持与同公司的终端检测防御系统联动，实现安装了终端检测防御系统的终端才能入网，没有安装的不允许入网。 |
| 25 | 阻断记录 | 支持防火墙模块阻断、流量模块阻断、行为管控模块阻断记录（提供截图证明） |
| 26 | 告警日志 | 支持非法网站、违规帖子、ftp上传、网页上传、违规邮件、违规im内容、以及匹配潜在威胁的记录。 |
| 27 | 会话日志 | 支持所有访问的会话日志记录，包括: 源 IP、目的 IP、协议类型、七层应用名称、源端口、目的端口、是否进行 NAT 转换(可显示转换后的 IP 和端口)、会话产生的时间和会话持续时间. （提供截图证明） |
| 28 | 个人统计分析 | 基于个人的所有行为监控报表，包括：网页标题记录、发贴记录、网页评论记录、在搜索引擎上的搜索记录、网页文件上传记录、URL访问记录、即时通讯的登录信息/聊天内容/文件传输记录、邮件记录（详细内容、附件）、FTP登录信息/上传记录/下载记录；（提供截图证明） |
| 29 | IPV6 | 支持IPv4和IPv6在一个系统版本内，同时支持V4和V6网络；支持接口配置ipv6地址、支持ipv6地址簿、支持ipv6策略路由、NAT64、NAT66、DNS64等相关配置 |
| 支持ipv6流量审计 |
| 支持ipv6环境下认证、流量控制、行为控制和防火墙策略 |
| 30 | 工作效率分析 | 针对员工在工作时段的浏览内容、访问应用的特征进行时长统计，根据预定义的规则判定员工的低效工作状态和时长。针对工作效率低下的员工，可以详细查看具体上网的网站和应用，以及时长，判定消极怠工有据可查 |
| 31 | ★日志外发 | 系统能够支持多个Syslog等第三方日志服务器系统。（需要提供截图） |
| 支持与任子行、派博、烽火、爱思、新网程、网星传媒、恒邦、白虹网监，中科新业、城安、上海创多、网星传媒、锐捷ELOG、兆物、亚美、网博、宽广智通、携网科技接口、华博接口、武汉洪旭接口、智开科技等20种以上的网安平台对接。 |
| 支持将用户行为日志上传到集中管理平台 |
| 32 | 失陷主机检测 | 支持对内网用户的主机进行分析，判断是否具有挖矿、勒索病毒、垃圾邮件行为等，分为高位和潜在区分。 |
| 33 | 违规告警分析 | 支持用户上网过程中的告警分析，以折线图和饼状图等多角度，罗列违规用户和行为记录，展示给管理员。 |
| 34 | 资质要求 | 具备全球IPv6测试中心《“IPv6 Ready Phase-2”认证》认证证书；产品具备公安部信息安全产品检测中心《互联网公共上网服务场所信息安全管理系统检测报告》；厂商具备中国信息安全评测中心颁发的信息安全服务（风险评估类二级）资质证书；厂商具备中国电子工业标准化技术协会颁发的信息技术服务运行维护标准符合性证书（运行维护），需提供证书复印件设备生产厂家具备信息系统建设及服务能力优秀级（CS4）等级证书；具备能力成熟度CSA CS-CMMI5认证；投标时需提供以上资质证书复印件； |
| 35 | ▲功能测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备工程中无法实现所需的功能，中标后要求投标方提供所投产品对技术指标要求的功能进行逐项测试验证，测试所产生的相关费用由投标方承担，若中标产品未通过测试，将取消中标资格并追究相应责任。 |
| 36 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. VPN

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | ▲性能要求 | 1U,千兆电口≥4个,标配单电源,整机吞吐≥800M，并发连接≥50万，IPSEC吞吐≥60M，SSL吞吐≥120M，SSLVPN配置授权20个，最大并发用户数≥300 |
| 2 | SSL VPN | 管理员分级分权管理，根据不同管理可以管理不同的功能模块；基于用户、用户组、用户角色进行授权，实现用户可访问资源、可信接入和客户端杀毒策略； |
| Windows、iOS、Android、Linux、Mac客户端和浏览器无控件接入方式； |
| ★支持可信接入功能，能够对接入主机的信息进行检查，包括域名、杀毒软件、必须安装的程序、必须运行的服务等（提供截图）；支持可信接入分级授权；支持检查策略：接入前检查、接入后检查、定时检查；支持移动应用白名单，只有白名单中的应用，才可访问内网资源； |
| 支持PC终端病毒查杀功能，综合传统的特征码技术和主动的启发式分析技术以及基于行为分析的病毒查杀技术，保护移动设备远离病毒、间谍软件、木马、蠕虫、bots等威胁的侵害；支持用户可自行配置终端类型，扫描级别等信息； |
| 内置CA，可以对证书进行生成、签发、废弃操作；支持国际、国密算法证书；支持DER/PEM/PKCS12等多种证书编码；支持导入多个第三方CA根证书和CRL列表，可以对不同的CA用户证书进行身份认证。支持通过HTTP协议定时下载同步CRL列表；支持支持通过OCSP/LDAP等协议对CA证书进行在线认证； |
| 支持AES、DES、3DES、RC4、MD5、SHA1、RSA等多种算法；支持国家商密专用的SM2、SM3、SM4算法；★支持国密、国际算法切换（提供截图证明）；支持高效流压缩算法； |
| PC端支持静态用户名口令、数字证书、短信、硬件特征码绑定、图形码、二维码扫描、指纹认证方式；支持使用RADIUS、TACACS/TACACS+、LDAP、域认证第三方安全认证方式；无需采购三方产品即可实现移动端支持人脸识别认证方式；支持两种或两种以上组合认证方式；（提供截图证明） |
| 支持Android及IOS移动应用中调用SSL VPN的SDK；支持移动APP自动封装SSL VPN的SDK； |
| 支持会话功能，能够实时监控在线用户的登录时间、登录IP、在线时间、访问流量，登录设备等多种信息； |
| 3 | IPsec VPN | 支持DES、3DES、AES、MD5、SHA1、DH GROUP1/2/5、RSA 1024/2048等加密算法；支持国家商密专用的SM2、SM3、SM4算法；支持高效数据流压缩算法； |
| 支持虚拟路由、隧道转发；支持使用标准的X.509证书建立隧道；支持多机多隧道的负载均衡和备份；支持网状、树型、星型等多种VPN网络拓扑； |
| 支持DDNS动态域名注册；支持使用域名进行隧道定义及协商；支持使用域名向TP进行集中认证；支持远程用户通过L2TP接入； |
| 4 | 业务监控 | 产品能够对设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC隧道状态、用户流量、安全事件、中国任意省市区县的接入用户数监控，并通过图表展示；（提供截图证明） |
| 5 | 安全策略 | 支持基于源/目的IP地址、MAC地址、端口和协议、时间、用户、角色的访问控制；支持基于状态检测的动态包过滤；支持隧道内的访问控制；支持动态端口协议：SIP、FTP、RTSP、SQL\*NET、MMS、RPC、TFTP、PPTP； |
| 支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换；支持双向NAT； |
| 6 | ★系统架构 | 为保障系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合TL9000-HSV R5.0/5.0标准，提供相关证明； |
| 7 | 系统管理 | 支持基于IP探测的链路备份功能；支持双机热备，连接保护模式；支持服务器的负载均衡，提供轮询、加权轮询、最少连接、加权最少连接、源/目的地址HASH等多种负载均衡方式；支持SNMP 的v1 、v2 、v2c 、v3 版本；支持SNMP MIB扩展；与当前通用的网络管理平台兼容，如HP Openview 等；支持系统故障自动切换和抢占功能； |
| 支持授权漂移策略，在主备模式下仅需采购一套接入许可； |
| 支持对配置文件的备份、下载、删除、恢复和上载；支持对部分配置本地和异地的批量导出和导入； |
| 8 | 资质要求 | 产品具备Ipv6 Ready认证资质；原厂商为国密局制定的《Ipsec技术规范》和《SSL VPN技术规范》起草单位；厂商具备中国电子工业标准化技术协会颁发的信息技术服务运行维护标准符合性证书（运行维护）；设备生产厂家具备信息系统建设及服务能力优秀级（CS4）等级证书；具备能力成熟度CSA CS-CMMI5认证；投标时需提供以上资质证书复印件； |
| 9 | ▲功能测试 | 为防止投标方虚假应答技术指标，从而造成用户在实际使用设备工程中无法实现所需的功能，中标后要求投标方提供所投产品对技术指标要求的功能进行逐项测试验证，测试所产生的相关费用由投标方承担，若中标产品未通过测试，将取消中标资格并追究相应责任。 |
| 10 | 服务 | 五年原厂质保，并提供原厂五年质保承诺函影印件 |

1. 综合运维管理平台

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 系统平台 | 基于Java平台开发，部署在Windows或linux平台上，同时支持国产化中标麒麟、UOS等操作系统。B/S模式，支持多采集器分布式部署。★系统登入方式采用二维码扫描的方式登入，并且支持微信和钉钉的同时登入。（需原厂提供功能截图并盖章） |
| 2 | 资产管理 | 1、整合的资源监控和管理模块,融监控、CMDB、报表、快照、知识库、体验化于一体。2、★CMDB可以管理设备的保修和服务信息，及时提醒用户续保，展现设备的图片信息和物理信息。支持二维码扫码查看功能，扫码即可查看设备的详细情况，并且在巡检时扫二维码即可查看信息。（需原厂提供功能截图并盖章）提供快照功能，把网络异常瞬间的各个设备和资源的情况生成快照。 |
| 3 | IPV6支持 | 支持在IPv4和IPv6双栈环境和过渡架构下实时监控，IPV6单设备发现，实现统一平台监控和管理 |
| 4 | 综合管理 | 1、跨厂商、跨平台，集网络设备、服务器、数据库、中间件、服务、防火墙、安全设备、光纤交换机等各种软硬件实现一体化监控，提供统一告警信息，智能的异常策略。2、提供快照功能，用户可以把网络异常瞬间的各个设备和资源的情况生成快照，以便后续对指标和关联性逐项分析。可以监控、CMDB、报表、快照、知识库、体验化于一体，无需各模块切换，支持设备的批量操作，导入、导入、删除、配置、地域、管理状态、关键状态、管理人等功能。 |
| 5 | 网络管理 | 对支持SNMP协议的交换机、路由器、防火墙、均衡负载等设备监控。1、监管内容包括端口状态、流量、端口错包率，端口丢包率等信息。2、网络设备接口监控，实时检测每个端口的上下行速率利用率 丢包率 包长等，自动识别端口所属VLAN,及与上联设备的连接关系和容量。 |
| 6 | 面板展现 | 直观展现设备真实背板情况及设备接口的连接信息，可以对设端口进行实时查看、打开和关闭等操作，能及时查看各个端口的基本信息,接口列表可监控指标当前值。当某个交换机出现异常速率或者异常流量时，能够提醒及时把相对应的端口宕掉。 |
| 7 | 服务器管理 | 1、支持监控多种主流操作系统，包括Windows、Linux AS、AIX、Solaris、HP-UX等。操作系统的详细信息，包括多个CPU中每个CPU的实时负载情况。2、硬件管理监控，主板、CPU、内存、系统磁盘、风扇状态、电源状态、网卡状态等硬件监控。支持通过自定义SNMP OID 脚本，采集特殊的服务器特殊指标项。支持通过自定义SNMP OID 脚本，采集特殊的服务器特殊指标项。（需原厂提供功能截图并盖章） |
| 8 | 数据库监控 | 1、支持的数据库类型sqlserver2005,sqlserver2008,sqlserver2012,oracle、mysql等。2、对表空间进行容量规划，表空间的使用情况进行定期分析和预警；实时监控当前数据库连接、监听器的管理并能够在连接数据库出现问题时告警；对数据库的碎片情况进行监测；对SQL 的执行效率进行分析；4、数据库的监控包括配置的连接监控、语句的执行情况监控、数据库的性能及其阀值的监控。5、数据库监视器实例对数据库连接失败、执行语句失败、性能阀值越界产生报警事件。 |
| 9 | 中间件监控 | 1、支持的中间件类型tomcat ,DB2,IIS,apache,tuxedo, jboss, weblogic, websphere等。2、通过模拟监视和性能指标两种方式进行：实时监控当前中间件的连接响应时间、监听器的管理模式，能够在连接中间件出现问题时告警检测。监控中间件的响应时间、请求数、传输速度、内存总数、连接数、收到字节数、发送字节数、总请求数、发生错误请求数等等诸多指标，并可直观了解所在服务器的性能和使用情况 |
| 10 | 服务管理 | 监控网页、邮件、文件、DNS等服务 ，监控响应时间、状态码、服务健康度、可用率、日志分析。服务应用运行情况监控以及服务管理等内容监控 |
| 11 | 指标系统 | 1、提供指标系统，包括通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标、配置指标等等。2、设置不同类型指标的轮询周期、阈值、异常策略、告警方法、异常过滤方法和告警过滤方法。3、支持设置多阈值策略，可设置交集或并集阈值策略，以适应多种设置场景以避免遗漏特殊告警。4、用户可以自定义SNMP采集器、SQL采集器、Tcp采集器来采集各种系统的各个实时指标，并在拓扑图、实时运行情况等等界面展现。 并能提供实时健康度和可用率等等服务水平相关指标。5、★支持指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤。可自定义ssh、telnet、SNMP、tcp、SQL、ping取值，SSH取值和TELNET取值在同一模块中，提供SSH和telnet取值模版和方式不低于15个模版，snmp、sql模版不低于5个（需提供原厂功能截图并盖章） |
| 12 | 模板管理 | 1、提供通过“模板”来设置指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤。2、通过模板设置通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标和配置指标等等。3、提供各种内建模板，包括SNMP网络设备模板、Windows2003模板、Windows2008模板、LinuxAS4模板、LinuxAS5模板、HP-UX基本模板、HP-UX告警模板、AIX基本模板、AIX高级模板、防火墙模板、Oracle数据库模板、SQLserver数据库模板、各中间件模板等等。 |
| 13 | 智能基线 | 1、采用大数据分析和AI自动学习能力，根据历史运维数据自动生成标准基线，形成高负载与低负载的运行规律。 2、系统提供智能化模板告警策略，根据各自设备自动建立基线数据。3、基线告警后，系统在详细页中展示过去的历史曲线，定位故障点第一时间数据。 |
| 14 | 拓扑展示 | 1、自动生成物理拓扑图。支持自定义灵活部署物理、示意、业务、及机柜拓扑图等，以可视化动态展现资源的结构分布、链路关系、性能指标和运行状态等，并能通过颜色策略、动态流量、告警提示变化来表示每个资源的异常等级2、布局至少包括（径向类、树状、坐标类、蜗牛状等）类型，图片布局至少包括（图片类、失量图元、图片鱼眼、小圆点类、小圆点鱼眼等）类型，链路样式至少包括（默认、直线、流量光速、方向箭头、方向气球、正交、流模式、贝塞尔曲线、磁线）等类型。3、拓扑支持分层分级展现，支持收缩设置父子级的关系，可快速进入下线拓扑，方便运维人员进行操作及查看，同时支持在同一拓扑图中，支持建立分区，分组，收缩和展开，以及链路合并功能，且能够在收缩的情况下，看到下级的异常情况，并指示灯和数字提醒。拓扑图支持鹰眼功能，方便大环境平移直观查看。（需提供原厂功能截图并盖章）4、支持页面添加文字和区域框并自动拉伸，以及颜色调整，支持各行业和各省地图背景专业图库，适用于多种场景，并支持上传图元背景。 |
| 15 | 个性化定制 | 1、在一个页面上提供系统总览、异常一览、报表一览、我的关注。把多个重要的监控类型设为我的关注，显示这些设备的实时运行情况和历史运行情况。2、提供“我的”界面。在一个页面上配置多个组件，支持第三方界面直接嵌入。可以自行定义页面轮换间隔时间（如15秒、30秒、40秒、1分钟、2分钟、3分钟、5分钟）。（需原厂提供功能截图并盖章）3、系统可以自动在多个界面自动轮换，包括整体页面、我的页面、故障页面、分析页面。提供换肤功能，至少4种不同界面风格。 |
| 16 | 告警方式 | 1、支持多种告警方式，消息框告警，声音，短信，邮件等方式并进行多种组合。2、平安通知，系统自带自检测功能，可定时通知网管平台运行情况，做到平台稳定性自检测，确认网络故障信息及时通知用户 |
| 17 | 异常处理 | 1、可自动判断偶然波动，避免误报事件2、对不同的异常和告警生成过滤条件并进行过滤3、系统在一段时间内对连续性的同一故障只报一次警，避免告警风暴4、支持故障智能依赖树配置，找出故障真正的来源，系统能够通过异常依赖树智能分析各个异常间的逻辑关联关系，提供根本原因分析 |
| 18 | 报表和订阅 | 1、报表系统支持自定义和内建报表模板，模板可以分为内建、公共、个人、共享模板；2、报表支持订阅、退订；3、报表种类有日周月年报表和快照报表和一日内不同时段报表；4、运行周期有一次性报表和周期性报表。 |
| 19 | 分析和统计 | 1、报表可以实时统计分析每次轮询数据、30分钟统计、2小时统计、日统计等多种实时统计和数据保存。2、同时展现各指标的轮询统计数据，分成日周月年曲线进行图形趋势分析。3、自定义时间段分析各个指标的历史情况。4、支持多设备多指标分析，用户可以对多个设备的多个指标在指定的同一个时间段内进行对比分析，并导出到Excel。  |
| 20 | 智能巡检 | 1、支持按不同巡检内容和设备制定周期性的定点智能巡检,自定义添加检测点,构建巡检规则。2、以模板规范标准值为依据,根据预设的要求进行数据采集,进行自主分析判断,进行定期巡检。 3、以报表的形式直观反映巡检结果,将巡检异常状态以告警灯形式展现,快速反映本次巡检的异常, 越界次数、标准值和当前值的差异性,系统会定期生成并主动发送运维人员。4、支持对系统监控巡查的整体进行评价和备注说明,导出多种格式向领导汇报。 |
| 21 | 故障分析 | 1、系统可以方便用户实时查看系统中的不同异常类型，并能筛选出不同状态2、在查看和筛选时，同一屏幕上，可以通过立体饼图和立体柱状图动态展现不同等级和不同种类异常的各项分类数据和总数。 |
| 22 | 个性化定制 | 用户可以通过个性化设置，简单在界面上定制用户的单位名称、系统名称  |
| 23 | 地域和权限管理 | 不同的操作员角色应可以灵活的分配展现内容，不同角色的操作员登录后只展现该角色权限允许的监控管理界面。 |
| 24 | 日志管理 | 记录设备管理用户登录登录设备成功或失败信息，包括登录名、登录结果（失败原因），登陆时间，日志类型等，日志可以导出到Excel表格中。 |
| 25 | 系统备份与恢复数据维护 | 1、支持检测和查看数据类型的范围和容量。支持数据备份结束以客户端和消息进行通知。支持下载数据到任何终端。通过核心数据存储设置，自定义保留用户最为关心的数据指标。2、支持一键备份与定时备份功能。支持一键恢复和上传数据恢复。（需原厂提供功能截图并盖章）3、对系统性能数据、异常数据、报表数据、日志数据进行当前容量的检测，并可设置超过阈值告警方式，执行立即清理功能。 |
| 26 | 网元数量 | 可管理网络设备、服务器、数据库、中间件、服务资源、网页资源、安全设备管理100网元 |
| 27 | 测试要求 | 中标候选人在签订合同前需到实地考察网络情况，并根据招标要求提供最新软件对以上功能进行逐一测试，测试通过方可签订合同。如测试发现有虚假应标情况，做废标处理并追究相关责任和赔偿。 |
| 28 | 原厂商服务 | ★在投标时必须提供原厂商5年免费服务承诺函原件。服务期内提供软件免费升级和维护；软件升级、软件故障问题，提供7\*24小时的项目专项电话技术支持（提供原厂商服务承诺函）原厂商产品为具有自主知识产权的国产网管系统。原厂商产品具有与国产化达梦数据库的互认证书原厂商产品具有与国产化东方通中间件的互认证书原厂商产品具有与国产化人大金仓数据库的互认证书原厂商产品具有与国产化中科曙光的互认证书厂商产品具有与国产化统信服务器的互认证书原厂商产品具有与国产化达南大通用数据库的互认证书原厂商产品具有与国产化银河麒麟服务器的互认证书原厂商产品具有与国产化金蝶天燕中间件的互认证书原厂商产品具有与国产化凝思操作系统的互认证书原厂商产品具有与国产化中科可控操作系统的互认证书原厂商产品具有与国产化中兴新支点操作系统的互认证书原厂商产品具有与国产化普华操作系统的互认证书原厂商产品具有公安部检测报告产品厂家要求具有ITIL认证工程师证书3名，并在投标时提供相关认证证书扫描件并盖章，并由原厂工程师完成实施和后续服务。 |

1. 精密空调

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标要求** |
| 1 | 机房精密空调 | 1、风冷模块化空调，可拆分的模块化结构设计，方便进场搬运，并可现场组装，制冷量（KW）≥40.5，显冷量(KW) ≥37.1，压缩机类型：涡旋式；2、提供精密空调制造厂商生产许可证、ISO9001证书，且产品获得CRAA认证证书、CE认证证书、CQC节能认证证书及整机ROHS环保报告；3、提供原厂经国家压缩机制冷设备质量监督检验中心认证的焓差实验室证书，证书制冷量范围需涵盖4~270kw；4、控制器采用7寸彩色液晶触摸屏显示器，能显示温湿度，具有图形显示机组内各组件的运行状态的功能，易操作的人性化界面，全中文背光显示。精密空调内部控制器不得采用第三方品牌，必须为自主研发产品，避免专利纠纷，需具备同品牌控制系统主控制软件著作权证书；5、机组采用静电地板下送风，标配电子可调速且节能的EC风机，送风量(m3/h)≥10600，机组送风余压20～300 Pa现场可调节；6、温度范围和精度 17-32±1℃，湿度范围和精度40-70±5%RH，温、湿度波动超限应能发出报警信号；7、精密空调报警记录储存量不少于500条；8、加热量（KW）≥9，采用多级电加热；9、显热比 ≥0.91、能效比 ≥3.1；10、可反复拆卸清洗的电极式加湿器，加湿量≥5kg/h；加湿器具备自动定时排水控制功能，极大减少加湿器维护工作量，提供原厂加湿控制软件著作权证书并加盖原厂公章证明；11、空调采用低噪音设计的特性，提供节能静音型精密空调相关证书文件证明；12、因机房进场及摆放空间有限，空调机组采用模块化结构方便进场搬运，并需具有较小尺寸，单模块最大尺寸长×宽×高（mm）≤875mm\*990mm\*1980mm，整机尺寸长×宽×高（mm）≤1325mm\*990mm\*1980mm；13、室外机提供冷凝风扇无级变速控制器，由电脑控制器根据冷凝压力控制执行调速运行；14、精密空调需配置RS485通信接口，提供通信协议，方便接入机房动力环境监控系统进行监控；15、精密空调原厂商需具备完善的售后服务体系及良好的售后服务能力，提供GB/T 27922-2011商品售后服务评价体系认证证书，证书涵盖范围须包括：机房专用精密空调的售后服务，且认证等级达到五星级。 |
| 2 | 室内机支架 | 槽钢按需定制 |
| 3 | 室外机支架 | 槽钢按需定制 |
| 4 | 空调主机输入电缆 | 4\*16+1\*10(平方），市电输入到UPS主机电缆与UPS输出到配电箱电缆,约30米 |
| 5 | 室外机电力线 | 3\*2.5(㎡)约30米 |
| 6 | 铜管 | 液管22/汽管25 30米 |
| 7 | 排进水管 | 管径与精密空调功率匹配约10米 |
| 8 | 精密空调安装 | 空调安装：铜管保温、制冷剂、排水、焊接工艺等 |
| 9 | 辅材 | 搬运上楼，调试，墙体打洞，安装时所必需的铜鼻子，绝缘管等 |
| 10 | 服务 | 提供五年原厂质保 |

1. 数据中心系统割接、数据迁移和机房设施

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **机房** | **设备材料名称** |  **主要技术参数** | **单位** | **数量** |
| **一、机房装修** |
| 1 | 信息机房 | 地板下防尘防静电涂料 | 地面漆面处理二遍 | m2 | 94 |
| 2 | 信息机房 | 抗静电地板 | 600\*600\*35mm，含支架，集中载荷≥550KG | m2 | 72 |
| 3 | 信息机房 | 地板收边压条 | 40\*4角钢 | m | 54 |
| 4 | 信息机房 | KVM | 16口数字式kvm 带17.3寸折叠液晶 1080P分辨率,含16个VGA+USB模块,支持16路远程IP访问 | 台 | 1 |
| 5 | 信息机房 | 金属踢脚线 | 1.0厚不锈钢踢脚线1、参见13J502-3图集N04-32、满足A级防火要求3、详见材料表，轻质隔墙节点图-2 | m | 54 |
| 6 | 信息机房 | 风口地板 | 空调出风地板，600\*600\*35mm | 块 | 24 |
| 7 | 信息机房 | 机柜承重架 | 采用镀锌材料根据机柜尺寸定制，8#槽钢  | 套 | 24 |
| 8 | 信息机房 | 精密空调主机承重架 | 采用镀锌材料根据机精密空调主机尺寸定制，8#槽钢， | 套 | 2 |
| 9 | 信息机房 | 精密空调室外机承重架 | 采用镀锌材料根据机精密空调外机尺寸定制，水泥基础，5#角钢， | 套 | 2 |
| 10 | 信息机房 | 市电配电柜 |  成套 ：市电输入配电柜，配置1个320A/3P总空气开关， 内含精密空调接入：63a/3p\*2个，32a/3p\*1个，市电接入：200a/3p\*1个，备用：100a/3p\*1个，63a/3p\*1个，24个服务器机柜接入：16a/1p\*24个，备用：16a/1p\*4个，需配置智能电量仪及防浪涌保护器，包括柜体、铜排及所有辅材，空开要求选用品牌：施耐德/abb/西门子 | 套 | 1 |
| 11 | 信息机房 | 市电配电柜承重架 | 采用镀锌材料根据机精密空调尺寸定制，5#角钢 | 套 | 1 |
| 12 | 信息机房 | 精密空调电缆 | ZR-YJV-4\*16+1\*6mm2 | m | 60 |
| 13 | 信息机房 | 机柜电缆 | YJV4X6+1X4 | m | 700 |
| 14 | 信息机房 | UPS配电柜增加空开及移位 | 配电柜移位，增加32A/1P空开\*12及配件，成套 | 套 | 1 |
| 15 | 信息机房 | UPS配电柜承重架 | 采用镀锌材料根据机精密空调尺寸定制，5#角钢 | 套 | 1 |
| 16 | 信息机房 | 桥架 | 300\*100mm环保镀锌网格桥架，Q235材质，钢丝直径5MM | m | 20 |
| 17 | 信息机房 | 桥架 | 强电封闭式防火桥架，100\*50\*1.2，含接地 | m | 20 |
| 18 | 信息机房 | 机柜专用PDU | 8位 ，防雷PDU | 条 | 34 |
| 19 | 信息机房 | 服务器机柜 | 1.尺寸大小：宽600mm\*深1200mm\*高2000mm2.机柜容量：42U3.颜色：黑色4.材料：优质冷轧钢板；机柜结构：拼装式机柜机架5.前面：单开玻璃门，后门：单开钢板门，机柜侧板：两块侧板可拆卸6.规格厚度：19英寸角规2.0，框架1.2，其他1.27.负载：动态 ≤600；静态≤10008.表面脱脂、磷化、静电喷塑处理，19英寸角规镀锌9.最大开启角度：＞180度，防护等级：IP20 | 台 | 8 |
| 20 | 信息机房 | 服务器机柜 | 1.尺寸大小：宽600mm\*深1000mm\*高2000mm2.机柜容量：42U3.颜色：黑色4.材料：优质冷轧钢板；机柜结构：拼装式机柜机架5.前面：单开玻璃门，后门：单开钢板门，机柜侧板：两块侧板可拆卸6.规格厚度：19英寸角规2.0，框架1.2，其他1.27.负载：动态 ≤600；静态≤10008.表面脱脂、磷化、静电喷塑处理，19英寸角规镀锌9.最大开启角度：＞180度，防护等级：IP20 | 台 | 2 |
| 21 | 信息机房 | 智慧大屏 | 显示器参数： 1、65寸，分辨率 3840\*2160 4K高清 2、可视角度：178° 3、触控点数：20点触控 4 、响应时间≤0.08S 5、画面比例：16：9 6、触控精度≤3.3mm 7、识别原理 ：红外识别 8、屏幕硬度：钢化防爆玻璃 ops参数： 1、CPU：≥Intel酷睿I7； 2、内存：≥8GB DDR3及以上；3、硬盘：≥SSD256G固态硬盘； 4、内置系统：正版windows10 5接口：≥4路USB、≥1路RJ45网络接口、≥1路麦克风输入、≥1路HDMI输出。 机器端口 ： 1、输入端子：≥2路 USB3.0；≥1路USB2.0；≥1路HDMI IN；≥2路Type-C；≥1路RS232；≥1路TOUCH， 2、输出端子：≥1路 AUDIO OUT  | 套 | 1 |
| 22 | 信息机房 | 壁挂支架 | 65寸壁挂支架 | 套 | 1 |
| 23 | 信息机房 | 办公电脑 | I7-10700F/8G/256G+1TB/R5-430 2G/WIN10H/5年上门/21.5\*1 | 台 | 1 |
| 24 | 信息机房 | 操作台 | 操作台主体框架需采用不小于厚度为1.5mm,优质冷轧镀锌钢板折弯横梁组合而成。台面和侧板为高密度豪华烤漆板，造型颜色根据需求定制；设备柜内不可有刮手的利口，并且便于进行改造和扩充、且无需钻孔作业。柜体左侧设置主机柜，右侧设置文件抽屉柜，中间为空档，办事人员可伸脚，位置舒适。长度1500mm，台面宽度800mm，高780mmmm，配套键盘抽屉用于放置键盘鼠标，台面干净整洁。一工位，操作台台面前端为木质或者钢制屏风，颜色可定制，外表静电喷粉处理。整体效果美观大方实用。 | 台 | 2 |
| 25 | 信息机房 | 办公椅 | 配套操作台的办公椅，结实舒适 | 张 | 2 |
| 26 | 信息机房 | 辅材 | 网络线、数据连接线及安装辅材等 | 套 | 1 |
| **二、割接、数据迁移等集成** |
| 序号 | 信息机房 | 工作项目 | 工作内容 |
| 1 | HIS、EMR服务器搭建 | 原有数据库600G，两台物理机做RAC，做DG数据迁移 |
| 信息集成平台搭建 | 两台物理机做RAC，新建数据库 |
| 新建虚拟化集群 | 搭建VMware，把原有虚拟集群迁移至新建集群 |
| 影像存储 | 原有40T左右的影像数据，配合软件公司，做好数据迁移 |
| 利旧服务器 | 原有8台服务器做虚拟集群，用于备份服务器和调试服务器使用，并在灾备时能做临时服务器使用 |
| 网络优化 | 医共体网络一体化的搭建、调整（柯城区人民医院内容网、卫生专网等多种网络融合） |
| 数据备份 | 对重要数据进行实时备份，并在灾备时能做临时数据库使用 |
| 机房运维管理 | 新建运维软件，将各个信息要素收集呈现、管理机房、有预报警等功能 |

**四、总体商务需求**

2.1交货时间及地点

**▲(1)** 中标人应在合同签订之日起15日历天完成供货，供货后15日历天内完成安装、调试并验收合格

(2)交货地点：采购人指定地点。

(3)中标人提供的中标物品，必须符合本招标文件要求、原包装送达采购单位；如有不符，采购人可以无条件退货，所造成的损失由中标人承担。更换后的零部件质保期按更换日起顺延。

2.2质保期及售后技术服务要求

 **▲(1)质保期：5年全保。**

 (2)质量保证期内提供免费上门维护、升级服务，如设备出现故障，供货单位在接到电话后，立即响应，2小时以内到现场处理，12小时内修复，现场不能修复的，必须采取无偿提供采购物品的备用件或整机等措施，保证用户单位的正常使用。

(3)投标人应提供技术支持方案，内容由投标人根据实际选择以下要点：服务机构（维保点）的地址、人员状况、维修能力、联系方式、营业执照、公司资质材料、相关案例等。

(4)完整准确地表述原厂家的标准售后服务承诺（范围、标准及期限等）、投标人可能增加的服务承诺等。

**2.3.项目实施计划**

项目实施的组织工作方案：工作时间进度表、工作程序或步骤、管理和协调方法、送货方案等。

**▲2.4.付款方式**

中标人在合同签订前向采购人支付中标金额的3%作为履约保证金；设备安装调试验收合格后采购人支付全额货款，3%履约保证金转为质保金在正常使用一年后退还中标人。

**第四部分** **评标方法及评分标准**

**一、评标方法**

**1.综合评分法。**综合评分法，是指投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为中标候选人的评标方法。

**二、评标委员会的组成**

**2.评标委员会的组成。**评标委员会由评审专家组成，成员人数为5人以上单数。

**3.评标委员会的组成人员的回避。**在政府采购活动中，评标委员会的组成人员与供应商有下列利害关系之一的，应当回避：

　　3.1参加采购活动前3年内与供应商存在劳动关系；

　　3.2参加采购活动前3年内担任供应商的董事、监事；

　　3.3参加采购活动前3年内是供应商的控股股东或者实际控制人；

　　3.4与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

　 3.5与供应商有其他可能影响政府采购活动公平、公正进行的关系。

**三、评标委员会的职责**

**4.评标委员会负责具体评标事务，并独立履行下列职责：**

4.1审查、评价投标文件是否符合招标文件的商务、技术等实质性要求；

4.2要求投标人对投标文件有关事项作出澄清或者说明；

4.3对投标文件进行比较和评价；

4.4确定中标候选人名单，以及根据采购人委托直接确定中标人；

4.5向采购人、采购机构或者有关部门报告评标中发现的违法行为；

4.6法律、法规、规章、招标文件等规定的其它事项。

**5.评标委员会及其成员不得有下列行为：**

　5.1确定参与评标至评标结束前私自接触投标人；

　5.2接受投标人提出的与投标文件不一致的澄清或者说明（财政部87号《政府采购货物和服务招投标管理办法令第五十一条规定的情形除外）；

　5.3违反评标纪律发表倾向性意见或者征询采购人的倾向性意见；

　5.4对需要专业判断的主观评审因素协商评分；

　5.5在评标过程中擅离职守，影响评标程序正常进行的；

5.6记录、复制或者带走任何评标资料；

　5.7其他不遵守评标纪律的行为。

　　评标委员会成员有5.1-5.5行为之一的，其评审意见无效，并不得获取评审劳务报酬和报销异地评审差旅费。

**四、评审程序**

**6.符合性审查。** 评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。符合投标无效情形的，投标无效。

**7.投标人澄清、说明或者补正。**对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。

**8. 比较与评价。**标委员会应当按照评标标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

**9. 汇总（资信技术得分情况）。**评标委员会各成员应当独立对每个投标人的商务和技术文件进行评价，并汇总资信技术得分情况。

**10. 报价审核。**对经商务和技术评审符合采购需求的投标人的报价的合理性、准确性等进行审查核实。

10.1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。

10.2根据财政部发布的《政府采购促进中小企业发展管理办法》规定，对于非专门面向中小企业的项目，对小型和微型企业产品的价格给予一定的扣除，用扣除后的价格参与评审。

10.3投标价格的修正原则。投标文件报价出现前后不一致的，按照下列规定修正：

10.3.1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;

10.3.2大写金额和小写金额不一致的，以大写金额为准;

10.3.3单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价;

10.3.4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。

10.3.5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。

▲**投标人对根据修正原则修正后的报价不确认的，投标无效。**

**11.汇总得分。**评标委员会各成员应当独立对每个投标人的投标文件进行评价，并汇总每个投标人的得分。

**12.顺序排列与中标候选推荐。**

12.1评标结果按评审后得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。得分最高的投标人为排名第一的中标候选人。

12.2多家投标人提供相同品牌产品（单一产品采购项目中的该产品或者非单一产品采购项目的核心产品）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，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。

**13.投标无效。**有下列情况之一的，投标无效：

13.1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参加同一合同项下的政府采购活动的（均无效）；

13.2为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商再参加该采购项目的其他采购活动的；

13.3投标人不具备招标文件中规定的资格要求的（投标人未提供有效的资格证明文件的，视为投标人不具备招标文件中规定的资格要求）；

13.4如以联合体形式参加政府采购活动的，联合体协议不符合招标文件规定的联合体协议要求的；

13.5投标文件未按规定的格式编制的；

13.6投标文件未按招标文件的澄清、修改的内容编制，又不符合实质性要求的；

13.7投标文件组成漏项，内容不全或内容字迹模糊辨认不清的；

13.8投标文件中法定代表人授权书所载内容与本项目内容有异的；

13.9投标文件未按照招标文件要求签署、盖章的；

13.10**未传输递交电子投标文件的或者未按规定提供相应的备份投标文件，造成项目开评标活动无法进行下去的；**

13.11投标文件中未提供应当提供的政府强制采购节能品目内的节能产品或未提供有效的节能产品认证证书的（如果本项目采购涉及节能品目清单中的政府强制采购的节能产品的）；

13.12投标文件含有采购人不能接受的附加条件的；

13.13投标文件中承诺的投标有效期少于招标文件中载明的投标有效期的；

13.14投标人所投内容不符合采购需求中实质性要求的；

13.15投标文件出现不是唯一的、有选择性投标报价的;

13.16投标报价高于本项目采购预算或者最高限价的;

13.17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，未能按要求提供书面说明或者提交相关证明材料，不能证明其报价合理性的;

13.18《投标（开标）一览表》填写不完整或字迹不能辨认或有漏项的；

13.19投标人对根据修正原则修正后的报价不确认的；

13.20投标人提供虚假材料投标的（包括但不限于以下情节）；

13.20.1使用伪造、变造的许可证件；
   13.20.2提供虚假的财务状况或者业绩；
   13.20.3提供虚假的项目负责人或者主要技术人员简历、劳动关系证明；
   13.20.4提供虚假的信用状况；
  13.20.5其他弄虚作假的行为。
 13.21投标人有恶意串通、妨碍其他投标人的竞争行为、损害采购人或者其他投标人的合法权益情形的；有下列情形之一的，属于或视为恶意串通，其投标无效：

13.21.1供应商直接或者间接从采购人或者采购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；

13.21.2供应商按照采购人或者采购机构的授意撤换、修改投标文件或者响应文件；

13.21.3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；

13.21.4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；

13.21.5供应商之间事先约定由某一特定供应商中标、成交；

13.21.6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；

13.21.7供应商与采购人或者采购机构之间、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。

13.21.8不同投标人的投标文件由同一单位或者个人编制；

13.21.9不同投标人委托同一单位或者个人办理投标事宜；

13.21.10不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

13.21.11不同投标人的投标文件异常一致或者投标报价呈规律性差异；

13.21.12不同投标人的投标文件相互混装；

13.22法律、法规、规章（适用本市的）及省级以上规范性文件（适用本市的）规定的其他无效情形。

13.23根据法律、法规或招标文件要求，评标委员会认为应当作无效投标的其他情况。

**五、评标报告**

**14. 评标报告与推荐中标候选人。**评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告，并推荐中标候选人，评审报告由评标委员会成员签字确认提交。

**15. 评标争议事项处理。**评标委员会成员对需要共同认定的事项存在争议的，应当按照少数服从多数的原则作出结论。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。

**六、 废标**

**16.废标。**根据《中华人民共和国政府采购法》第三十六条之规定，在采购中，出现下列情形之一的，应予废标：

16.1符合专业条件的供应商或者对招标文件作实质响应的供应商不足3家的；

16.2出现影响采购公正的违法、违规行为的；

16.3投标人的报价均超过了采购预算，采购人不能支付的；

16.4因重大变故，采购任务取消的。

废标后，采购机构应当将废标理由通知所有投标人。

**七、 重新组织采购**

**17.修改招标文件，重新组织采购活动。**评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的，将停止评标工作，并与采购人、采购机构沟通并作书面记录。采购人、采购机构确认后，将修改招标文件，重新组织采购活动。

**18.重新开展采购。**有政府采购法第七十一条、第七十二条规定的违法行为之一，影响或者可能影响中标、成交结果的，依照下列规定处理：

18.1未确定中标或者成交供应商的，终止本次政府采购活动，重新开展政府采购活动。

18.2已确定中标或者成交供应商但尚未签订政府采购合同的，中标或者成交结果无效，从合格的中标或者成交候选人中另行确定中标或者成交供应商；没有合格的中标或者成交候选人的，重新开展政府采购活动。

18.3政府采购合同已签订但尚未履行的，或者无故不按规定时间供货的，撤销合同，从合格的中标或者成交候选人中另行确定中标或者成交供应商；没有合格的中标或者成交候选人的，重新开展政府采购活动。

18.4政府采购合同已经履行，给采购人、供应商造成损失的，由责任人承担赔偿责任。

18.5政府采购当事人有其他违反政府采购法或者本条例规定的行为，经改正后仍然影响或者可能影响中标、成交结果或者依法被认定为中标、成交无效的，依照18.1-18.4规定处理。

**八、评审过程的保密与录像**

**19.保密。**评审活动在严格保密的情况下进行。评审过程中凡是与采购响应文件评审和比较、中标成交供应商推荐等评审有关的情况，以及涉及国家秘密和商业秘密等信息，评审委员会成员、采购人和采购机构工作人员、相关监督人员等与评审有关的人员应当予以保密。

**20.录音录像。**采购机构对评审工作现场进行全过程录音录像，录音录像资料作为采购项目文件随其他文件一并存档。

**九、具体评标标准**

**21.评分办法**

**标项一：商务技术部分（70分）+价格分（30分）**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评分因素 | 评审标准 | 分值 |
| 1 | 报价 | 本项目最高限价473.3460万元，基准价为满足评标要求且投标价格最低的投标报价，报价得分=(基准价／投标报价)×30，四舍五入，保留两位小数。报价高于最高限价的，为无效投标文件。 | 30 分 |
| 2 | 类似项目业绩 | 投标人自2017年1月1日以来（以合同签订时间为准）签订的100万以上类似项目，每提供一个得1分，本项最高得5分。（须提供案例业绩证明材料，项目金额以中标通知书为准，清晰扫描件并加盖投标人公章，否则不得分） | 0-5分 |
| 3 | 资质证书  | 投标人具有ISO9001质量管理体系认证证书的得1分；投标人具有ISO14001质量管理体系认证证书的得1分；投标人具有浙江省安全技术防范三级证书及以上的得1分；投标文件中提供证书清晰扫描件加盖投标人公章，不提供不得分。本项最高得3分。 | 0-3分 |
| 4 | 项目组人员 | 要求项目经理具备PMP证书，得1分；项目组中有人员具有所投核心产品认证工程师证书的，每提供一名高级工程师得1分；每提供一名中级工程师得0.5分，中级工程师此处最高可得2分。本项最高得4分。须提供项目组人员社保缴费证明及证书清晰扫描件并加盖公章，否则不得分。 | 0-4分 |
| 5 | 售后服务方案 | 1、根据售后服务承诺的范围和完善程度（包括保修年限5年及以上的，保修部件范围，保修、服务标准，人员配备，故障响应修复时间方式及保障措施）综合打分。优得5-4分，良好得3-2分，一般得1-0分。2、供应商在衢州市设有生产基地或售后服务网点的得3分；在衢州市外浙江省内设有生产基地或售后服务网点的得2分；其他不得分；售后服务网点须提供有效的营业执照副本复印件及授权书。（0-3分） | 0-8分 |
| 6 | 培训 | 人员培训计划的合理性0-0.5分；承诺免费培训课程情况0-0.5分；培训时间、师资及方式0-1分；根据各投标人提供的培训方案完整性进行评定。 | 0-2分 |
| 7 | 技术方案 | 根据供应商提供的完整集成方案。方案设计的合理性、技术的先进性、稳定性、安全性、实际应用规模、对用户需求的理解程度、现场勘察程度等方面进行综合评分完善度酌情打分。项目涉及到数据迁移等关键业务割接，要求所有潜在中标人前期现场调研，取得用户正式确认盖章件。（此项为重要指标项）优得8-6分，良好得5-3分，一般得2-0分。 | 0-8分 |
| 8 | 配置参数 | 采购文件中采购需求部分打1、打“▲”号的为必须满足的关键性参数，不满足作无效标处理；2、除标“▲”号的参数外，“★”号的技术参数负偏离或缺漏项的每项扣0.5分，对非关键的性能指标及技术参数负偏离或缺漏项的每项扣0.3分，扣完为止。 | 0-25分 |
| 9 | 品牌情况 | 根据品牌知名度、用户使用情况反馈、好评度等情况酌情打分。优得3分，良好得2分，一般得1分。 | 0-3分 |
| 10 | 原厂质保承诺函 | 供应商提供原厂五年承诺函清晰扫描件并加盖公章，得2分，不提供不得分。 | 0-2分 |
| 11 | 设备可靠性 | 为保证整体项目后期运行稳定可靠以及整体服务质量，要求本次项目主要设备软硬件（存储、服务器）为同一品牌，提供硬件设备权威机构排名；为保证数据安全性，要求本次投标安全产品类，充分满足异构要求，要求涉及两个国内主流品牌。优得5-4分，良好得3-2分，一般得1-0分。 | 0-5分 |
| 12 | 总体设计 | 评标小组根据总体设计框架、业务流程和应用模式的先进性、安全性、稳定性、可扩展性等并结合考虑综合具体业务特色酌情打分。优得5分，良好得3分，一般得1分。 | 0-5分 |

投标文件中如附有外文资料，必须逐一对应翻译成中文并加盖投标人公章后附在相关外文资料后面，否则外文资料不予认可。翻译的中文资料与外文资料不符的，均不予认可。翻译严重错误的，将视同提供虚假资料。

23.其他需说明事项

无。

**第五部分 拟签订的合同文本**（以实际签订的合同为准）

（参考样本）

合同编号：

签订地点： 签订时间：20\* 年 月 日

项目名称：

甲方（需方）：

乙方（供方）：

供、需双方根据柯城区县域医共体建设-2021年基层医疗机构整体提升工程柯城区人民医院信息化提升工程（招标编号HBMDCG2021-055）招标结果和招标文件的要求，并经双方协调一致，订立本采购合同。

一、合同文件：

1、合同条款。

2、中标通知书。

3、招标文件。

4、更正公告。

5、中标单位投标文件。

6、其他。

二、合同金额:合同金额为(大写)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元（￥　　　　元）人民币。

附《采购项目清单内容》

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 采购项目 | 中标内容/品牌/型号 | 中标单价（元） | 数量 | 中标总价（元） |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |

三、质量要求及供方对质量负责条件和期限：

1、供方提供的货物必须是现货、全新，符合招标要求的规格型号和技术指标。供方对货物提供\*\*年的免费保修期（货物厂家另有超过此质保期的按原规定执行），保修期内非因需方的人为原因而出现质量问题的，由供方负责包修、包换或者包退，并承担调换或退货的实际费用。

2、供方在维保期内接到用户单位的电话后，在\*\*小时内响应，\*\*小时以内到现场，\*\*小时以内解决问题，不能修复的，必须采取无偿提供备品、备件或备机等措施，以保证用户单位的正常使用。

四、工期时间\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

交货地点：

五、货款支付

1、付款方式：

2、合同履行完毕，需方根据合同进行验收，验收合格后供应商按财政结算要求办理货款结算手续。

六、履约保证金

1、履约保证金：供方在签订合同时缴纳履约保证金，履约保证金金额为中标价的3%，履约保证金可以汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。合同开始履行，项目验收合格后转为质保金，在正常使用一年后退还供方。

七、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、乙方逾期交付货物的，乙方应按逾期交付货款总额每日千分之 五 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 日不能交货的，甲方自动解除本合同，履约保证金不予退还，如造成甲方损失超过履约保证金的，超出部分由乙方继续承担赔偿责任。

3、乙方所交的货物品种、型号、规格、技术参数、质量等不符合合同规定及投标文件承诺标准，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。

4、因需方原因逾期支付合同款，自逾期之日起，向供方每日偿付合同总价千分之 二的滞纳金；需方无正当理由拒付货款的，应向供方偿付合同总价百分之五的违约金。

5、如发现乙方违反招投标文件和合同的有关规定，甲方有权根据约定对乙方进行处罚，并有权提前终止合同。

八、调试和验收

九、争议的解决

因本合同引起的或与本合同有关的任何争议，合同双方应首先通过协商解决，达成书面协议，如协商不成，可选择下列第种方式解决。

（1）提请衢州仲裁委员会按照该会仲裁规则进行仲裁，仲裁裁决是终局的，对合同双方均有约束力。

（2）向有管辖权的人民法院提起诉讼。

十、合同生效

1、中标方持中标通知书作为与需方签订合同的凭证。

2、本合同经需、供双方法定代表人（符合浙财采监【2013】24号第六条规定的为负责人）或其授权委托人签名并加盖单位公章后生效。

需方（加盖公章）： 供方（加盖公章）：

地址： 地址：

法定代表人（或委托代理人）签名： 法定代表人（或委托代理人）签名：

联系电话： 联系电话：

邮政编码： 邮政编码：

开户银行： 开户银行：

帐号： 帐号：

 **第六部分 应提交的有关格式范例**

投标人按照以下格式编制投标文件，并将资格文件、报价文件、资信技术文件分别装订成册。

▲**资格文件部分**

**目录**

（1）营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，须提供自然人的身份证明）、税务登记证(或其它缴纳证明材料)复印件、社保登记证（或其它缴纳证明材料）复印件………………………………………………（页码）

（2）法人授权书 ……………………………………………………………………（页码）

（3）授权代表的身份证（复印件）………………………………………………（页码）

（4）最近一年年度资产负债表等财务报表资料文件(新成立的公司，提供情况说明)（页码）

（5）具有履行合同所必需的设备和专业技术能力的承诺函………………………（页码）

（6）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的声明 …（页码）

（7）具有良好商业信誉特别声明……………………………………………………（页码）

（8）符合特定资格条件（如果项目要求）的有关证明材料（复印件）…………（页码）

（9）以联合体形式投标的，提供联合体协议；本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供…………………………………………………（页码）

**一、营业执照或事业法人登记证证明材料（复印件）、税务缴纳证明文件（复印件）、社保缴纳证明文件（复印件）**

 投标人名称(电子签章)：

 日期： 年 月 日

**二、法人授权书**

XXX（采购单位名称或采购机构）：

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XXXXXXXX项目【招标编号：XXXXX】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。

 本授权书有效期：自 年 月 日起至 年 月 日止。

 特此告知。

 投标人名称(电子签章)：

 日期： 年 月 日

**联合体投标授权书（适用联合体投标），本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供**

兹委派公司先生/女士(其在该公司的职务是： ，联系电话：手机：传真：)；公司先生/女士(其在该公司的职务是： ，联系电话：手机：传真：)；……，代表本联合体全权处理\*\*\*\*\*项目【招标编号： 】政府采购投标的一切事项，若中标则全权代表本联合体签订相关合同，并负责处理合同履行等事宜。

 本授权书有效期：自 年 月 日起至 年 月 日止。

 特此告知。

单位： （电子签章） 单位： （电子签章）

日期： 年 月 日 日期： 年 月 日

**三、授权代表的身份证（复印件）**

身份证件扫描件：

|  |
| --- |
| 正面： 反面： |

 投标人名称(电子签章)：

日期： 年 月 日

**四、最近一年度资产负债表等财务报表资料文件（复印件）**

 投标人名称(电子签章)：

日期： 年 月 日

**五、具有履行合同所必需的设备和专业技术能力的承诺函**

XXX（采购单位名称或采购机构）：

我方郑重承诺，我方具有\*\*\*\*\*\*\*项目【招标编号：\*\*\*\*\*】合同所必需的设备和专业技术能力。如中标，我方将保证合同顺利履行。

 投标人名称(电子签章)：

日期： 年 月 日

**六、参加政府采购活动前三年内，在经营活动中**

**没有重大违法记录的声明**

XXX（采购单位名称或采购机构）：

我方声明投标截止时间前三年，在经营活动中没有重大违法记录。

**七、具有良好商业信誉特别声明**

XXX（采购单位名称或采购机构）：

截至投标截止时间，我方具有良好的商业信誉，不存在下列情形（包括但不限于）。否则，我方将承担在资格审查时不被通过的后果。

1**、**按照招标文件规定的信用信息查询渠道及截止时间，经查询列入失信被执行人名单、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；

2、截至投标截止时间，因违反《浙江省政府采购供应商注册及诚信管理暂行办法》而被列入‘黑名单’，在处罚有效期内。

 投标人名称(电子签章)：

 日期： 年 月 日

**八、特定资格条件要求的资质文件（复印件）**

（由投标人根据招标公告合格的投标人应具备的特定资格要求编制；如果本项目没有设置特定资格条件，则不需要提供）

**九、联合体协议（本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供）**

（以联合体形式投标的，提供联合体协议；本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供）

甲方：

乙方：

……

各方经协商一致，决定组成一个联合体，以一个投标人的身份就\*\*\*\*\*\*项目【招标编号：\*\*\*\*\*\*】共同投标。

一、各方一致决定，指定方牵头人，代表所有联合体成员负责投标和合同实施阶段的主办、协调工作。

二、所有联合体成员各方签署授权书，授权书载明的授权代表根据招标文件规定及投标内容而对采购人、采购机构所作的任何合法承诺，包括书面澄清及相应等均对联合投标各方产生约束力。

三、本次联合投标中，分工如下：甲方承担的工作和义务为：；乙方承担的工作和义务为： ；……

四、如果中标，联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

五、有关本次联合投标的其他事宜：

1、联合体各方不再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

2、联合体中有同类资质的各方按照联合体分工承担相同工作的，按照资质等级较低的供应商确定资质等级。

3、本协议提交采购人、采购机构后，联合体各方不得以任何形式对上述内容进行修改或撤销。

甲方单位： （电子签章） 乙方单位： （电子签章）

日期： 年 月 日 日期： 年 月 日

▲**报价文件部分**

**目录**

（1）投标响应函……………………………………………………（页码）

（2）投标（开标）一览表…………………………………………（页码）

（3）中小企业声明函………………………………………………（页码）

**一、投标响应函**

XXX（单位名称或采购机构名称）：

(投标人全称)授权(全权代表姓名)(职务、职称)为全权代表，参加贵方组织的XXXXXX项目【招标编号： 】招标的有关活动，并对此项目进行投标。为此：

1、我方同意在投标人投标人须知规定的开标日期起遵守本投标文件中的承诺且在投标有效期满之前均具有约束力。

2、我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商应当具备的条件：

(1)具有独立承担民事责任的能力；

(2)遵守国家法律、行政法规，具有良好的信誉和商业道德；

(3)具有履行合同的能力和良好的履行合同记录；

(4)良好的资金、财务状况；

(5)产品及生产所需装备符合中国政府规定的相应技术标准和环保标准；

(6)没有违反政府采购法规、政策的记录；

(7)没有发生重大经济纠纷和走私犯罪记录。

3、我方中标后拟在中标后将工作分包，分包承担主体是，我方承诺分包承担主体具备相应资质条件，且不再次分包。（不再将工作进行分包或本项目不允许分包的，下划线处填写“/”。）

4、提供投标人须知规定的全部投标文件。具体内容为：

(1)投标(开标)一览表；

(2)投标技术文件和商务文件；

(3)投标人须知要求投标人提交的全部文件；

(4)按招标文件要求提供和交付的货物和服务的投标报价详见投标(开标)一览表；

(5)保证忠实地执行双方所签订的合同，并承担合同规定的责任和义务；

(6)保证遵守招标文件中的其他有关规定。

5、我方承诺投标有效期从提交投标文件的截止之日起天，不少于招标文件中载明的投标有效期（从提交投标文件的截止之日起90天）。

6、我方完全理解贵方不一定要接受最低价的投标。

7、我方愿意向贵方提供任何与该项投标有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

8、我方已详细审核全部招标文件，包括招标文件修改书(如果有)、参考资料及有关附件，确认无误。

9、我方将严格遵守《中华人民共和国政府采购法》第七十七条规定，供应商有下列情形之一的，处以采购金额5‰以上10‰以下的罚款，列入不良行为记录名单，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吊销营业执照；构成犯罪的，依法追究刑事责任：

a)提供虚假材料谋取中标、成交的；

b)采取不正当手段诋毁、排挤其他供应商的；

c)与采购人、其它供应商或者采购机构恶意串通的；

d)向采购人、采购机构行贿或者提供其他不正当利益的；

e)在招标采购过程中与采购人进行协商谈判的；

f)拒绝有关部门监督检查或提供虚假情况的。

供应商有前款第a)至e)项情形之一的，中标、成交无效。

投标人名称（电子签章）：

 日期： 年 月 日

联系人：联系电话：

联系地址：

邮政编码：传真号码：

**注：未按照本投标响应函要求填报的将被视为非实质性响应投标，从而可能导致该投标被拒绝。**

二、投标(开标)一览表

 （单位名称或采购机构名称）：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：如你方接受本投标，我方承诺按照如下投标(开标)一览表的价格完成 项目【招标文件编号： 】，标项 的实施。

**投标(开标)一览表(单位均为人民币元)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **品牌（如果有）** | **规格型号（或具体服务）** | **数量** | **单价** | **总价** | **服务要求（年限）** |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
| **投标报价（小写）** |  |
| **投标报价（大写）** |  |

**注：**

1、投标人需按本表格式填写，不得自行更改。

2、有关本项目实施所涉及的一切费用（详见前附表）均计入报价。**采购人将以合同形式有偿取得货物或服务，不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务**，**各项明细费用请按实填写（不得出现“0元”“免费赠送”等形式的无偿报价）。**

3、以上表格要求细分项目及报价，在“规格型号（或具体服务）”一栏中，货物类项目填写规格型号，服务类项目填写具体服务。

4、特别提示：采购机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的的名称、规格型号、数量、单价、服务要求等予以公示。

5、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。注：投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

投标人名称（电子签章）：

 日期： 年 月 日

三、中小企业声明函（如有）

中小企业声明函（货物）

本公司（联合体） 郑重声明， 根据《政府采购促进中小企业发展管理办法》（财库﹝ 2020﹞ 46 号） 的规定， 本公司（联合体） 参加（单位名称） 的（项目名称） 采购活动， 提供的货物全部由符合政策要求的中小企业制造。 相关企业（含联合体中的中小企业、 签订分包意向协议的中小企业）

的具体情况如下：

1. （标的名称） ， 属于（招标文件中明确的所属行业）行业； 制造商为（ 企业名称）， 从业人员 人， 营业收入为 万元， 资产总额为 万元1， 属于（中型企业、 小型企业、 微型企业）；

2. （标的名称） ， 属于（招标文件中明确的所属行业）行业； 制造商为（ 企业名称）， 从业人员 人， 营业收入为 万元， 资产总额为 万元， 属于（中型企业、 小型

企业、 微型企业）；

……

以上企业， 不属于大企业的分支机构， 不存在控股股东为大企业的情形， 也不存在与大企业的负责人为同一人的情形。本企业对上述声明内容的真实性负责。 如有虚假， 将依法承担相应责任。

投标人名称（盖章/电子签章）：

日 期：

中小企业声明函（工程、 服务）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库﹝2020﹞46 号）的规定，本公司（联合体）参加 （单位名称） 的 （项目名称） 采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.（标的名称） ，属于 （招标文件中明确的所属行业） ；承建（承接）企业为 （企业名称） ，从业人员人，营业收入为万元，资产总额为万元属于 （中型企业、小型企业、微型企业） ；

2.（标的名称） ，属于 （招标文件中明确的所属行业） ；承建（承接）企业为 （企业名称） ，从业人员人，营业收入为万元，资产总额为万元，属于 （中型企业、小型企业、微型企业） ；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

投标人名称（盖章/电子签章）：

日 期：

**从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。**

 注：**投标人提供的中小企业声明函与实际情况不符的，投标价格不可享受价格扣除。**符合《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）规定的条件并提供《残疾人福利性单位声明函》（附件1）的残疾人福利性单位视同小型、微型企业；根据《关于政府采购支持监狱企业发展有关问题的通知》（财库[2014]68号）的规定，投标人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证明文件的，视同为小型和微型企业。

▲**资信技术文件部分**

**目录**

（1）营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为 自然人的，提供自然人的身份证明）………………………………………………（页码）

（2）联合体协议… …………………………………………………………（页码）

（3）资信文件复印件（如果要求提供） …………………………………（页码）

（4）主要业绩证明… ………………………………………………………（页码）

（5）其他商务文件或说明 …………………………………………………（页码）

（6）技术（服务）方案………………………………………………………（页码）

（7）技术（服务）偏离说明表…………………………………………………（页码）

（8）组织实施方案………………………………………………………………（页码）

（9）投标人的各项服务承诺 …………………………………………（页码）

（10）投标人认为需要的其他技术文件或说明……………………………（页码）

（11）关于对招标文件中商务、合同有关条款的拒绝声明…………………（页码）

**注：以上目录是基本格式要求，各投标人可根据自身情况进一步细化。**

1. **营业执照(或事业法人登记证或其他工商等登记证明材料)复印件（投标人为自然人的，提供自然人的身份证明）**

投标人名称(电子签章)：

 日期： 年 月 日

**联合体协议（本项目不接受联合体投标或者投标人不以联合体形式投标的，则不需要提供）**

甲方：

乙方：

……

各方经协商一致，决定组成一个联合体，以一个投标人的身份就\*\*\*\*\*\*\*\*项目【招标编号：\*\*\*\*\*】共同投标。

一、各方一致决定，指定方牵头人，代表所有联合体成员负责投标和合同实施阶段的主办、协调工作。

二、所有联合体成员各方签署授权书，授权书载明的授权代表根据招标文件规定及投标内容而对采购人、采购机构所作的任何合法承诺，包括书面澄清及相应等均对联合投标各方产生约束力。

三、本次联合投标中，分工如下：甲方承担的工作和义务为：；乙方承担的工作和义务为： ；……

四、如果中标，联合体各成员方共同与采购人签订合同，并就采购合同约定的事项对采购人承担连带责任。

五、有关本次联合投标的其他事宜：

1、联合体各方不再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

2、联合体中有同类资质的各方按照联合体分工承担相同工作的，按照资质等级较低的供应商确定资质等级。

3、本协议提交采购人、采购机构后，联合体各方不得以任何形式对上述内容进行修改或撤销。

甲方单位： （电子签章） 乙方单位： （电子签章）

日期： 年 月 日 日期： 年 月 日

**三、资信文件复印件（如果要求提供）**

（由投标人根据采购需求及招标文件要求编制）

 投标人名称(电子签章)：

 日期： 年 月 日

**四、主要业绩证明**

投标人名称（电子签章）：

 日期： 年 月 日

**五、****其他商务文件或说明**

（其他商务文件或说明由投标人根据采购需求自行编制）

投标人名称（电子签章）：

 日期： 年 月 日

**六、技术和服务方案**

（由投标人根据采购需求及招标文件要求编制）

供应商名称（电子签章）：

 日期： 年 月 日

**七、技术和服务偏离说明表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 采购要求 | 投标响应 | 偏离 | 说明 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

投标人名称（电子签章）：

 日期： 年 月 日

**八、组织实施方案**

（由投标人根据采购需求及招标文件要求编制）

投标人名称（电子签章）：

日期： 年 月 日

**九、投标人的各项服务承诺**

（由投标人根据采购需求及招标文件要求编制）

投标人名称（电子签章）：

日期： 年 月 日

**十、投标人认为需要的其他技术文件或说明**

（由投标人根据采购需求自行编制）

投标人名称（电子签章）：

日期： 年 月 日

**十一、关于对招标文件中有关商务、合同条款的拒绝声明**

（由投标人根据采购需求自行编制）

投标人名称（电子签章）：

 日期： 年 月 日

# 附件

**附件1：**

**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（电子签章）：

 日 期：

**附件2：质疑函范本及制作说明**

**质疑函范本**

一、质疑供应商基本信息

质疑供应商：

地址：邮编：

联系人：联系电话：

授权代表：

联系电话：

地址： 邮编：

二、质疑项目基本情况

质疑项目的名称：

质疑项目的编号：包号：

采购人名称：

招标文件获取日期：

三、质疑事项具体内容

质疑事项1：

事实依据：

法律依据：

质疑事项2

……

四、与质疑事项相关的质疑请求

请求：

签字(签章)： 公章：

日期：

**质疑函制作说明：**

1.供应商提出质疑时，应提交质疑函和必要的证明材料。

2.质疑供应商若委托代理人进行质疑的，质疑函应按要求列明“授权代表”的有关内容，并在附件中提交由质疑供应商签署的授权委托书。授权委托书应载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.质疑供应商若对项目的某一分包进行质疑，质疑函中应列明具体分包号。

4.质疑函的质疑事项应具体、明确，并有必要的事实依据和法律依据。

5.质疑函的质疑请求应与质疑事项相关。

6.质疑供应商为自然人的，质疑函应由本人签字；质疑供应商为法人或者其他组织的，质疑函应由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

**附件3：投诉书范本及制作说明**

**投诉书范本**

一、投诉相关主体基本情况

投诉人：

地 址：邮编：

法定代表人/主要负责人：

联系电话：

授权代表：联系电话：

地 址：邮编：

被投诉人1：

地 址：邮编：

联系人：联系电话：

被投诉人2

……

相关供应商：

地 址：邮编：

联系人：联系电话：

二、投诉项目基本情况

采购项目名称：

采购项目编号：包号：

采购人名称：

采购代理机构名称：

招标文件公告:是/否 公告期限：

采购结果公告:是/否 公告期限：

三、质疑基本情况

投诉人于年月日,向提出质疑，质疑事项为：

采购人/采购代理机构于年月日,就质疑事项作出了答复/没有在法定期限内作出答复。

四、投诉事项具体内容

投诉事项 1：

事实依据：

法律依据：

投诉事项2

……

五、与投诉事项相关的投诉请求

请求：

签字(签章)： 公章：

日期：

**投诉书制作说明：**

1.投诉人提起投诉时，应当提交投诉书和必要的证明材料，并按照被投诉人和与投诉事项有关的供应商数量提供投诉书副本。

2.投诉人若委托代理人进行投诉的，投诉书应按照要求列明“授权代表”的有关内容，并在附件中提交由投诉人签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。

3.投诉人若对项目的某一分包进行投诉，投诉书应列明具体分包号。

4.投诉书应简要列明质疑事项，质疑函、质疑答复等作为附件材料提供。

5.投诉书的投诉事项应具体、明确，并有必要的事实依据和法律依据。

6.投诉书的投诉请求应与投诉事项相关。

7.投诉人为自然人的，投诉书应当由本人签字；投诉人为法人或者其他组织的，投诉书应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。