杭州市智慧电子政务外网（2024）项目

招标文件

**（电子招投标）**

编号:HZZFCG-2024-081

杭州市数据资源管理局

杭州市公共资源交易中心

二〇二四年四月二十五日

**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 评标办法

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

杭州市智慧电子政务外网（2024）项目招标项目的潜在投标人应在政采云平台（https://www.zcygov.cn/）获取（下载）招标文件，并于2024年5月16日10点30分00秒（北京时间）前递交（上传）投标文件。

**一、项目基本情况**

**项目编号：**HZZFCG-2024-081

**项目名称：**杭州市智慧电子政务外网（2024）项目

**预算金额（元）：**14490000

**最高限价（元）：**14490000

**采购需求：**杭州市智慧电子政务外网（2024）项目主要内容：服务内容分为以下3块内容：线路资源租赁服务，设备租赁服务，设备维保服务。本次项目目标是完成杭州市电子政务外网核心承载网服务租赁，此承载网将服务于全市电子政务网接入单位及相关机构，同时承担省区政务外网的纵向互联互通，是杭州市电子政务服务的基础。本项目服务周期为1年（2024年7月1日至2025年6月30日）。具体以招标文件第三部分采购需求为准，供应商可点击本公告下方“浏览采购文件”查看采购需求。

**合同履约期限：**本项目服务周期为1年（2024年7月1日至2025年6月30日）。

**本项目接受联合体投标：****是；****否**。

**二、申请人的资格要求：**

1. 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；

2. 以联合体形式投标的，提供联合协议(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) ；

3.落实政府采购政策需满足的资格要求：

无（注：不得限制大中型企业与小微企业组成联合体参与投标）；

专门面向中小企业

服务全部由符合政策要求的中小企业承接，提供中小企业声明函；

服务全部由符合政策要求的小微企业承接，提供中小企业声明函；

要求以联合体形式参加，提供联合协议和中小企业声明函，联合协议中中小企业合同金额应当达到 %，其中小微企业合同金额应当达到 %;如果供应商本身提供所有标的均由中小企业制造、承建或承接，并相应达到了前述比例要求，视同符合了资格条件，无需再与其他中小企业组成联合体参加政府采购活动，无需提供联合协议；

要求合同分包，提供分包意向协议和中小企业声明函，分包意向协议中中小企业合同金额应当达到 % ，其中小微企业合同金额应当达到 % ;如果供应商本身提供所有标的均由中小企业制造、承建或承接，并相应达到了前述比例要求，视同符合了资格条件，无需再向中小企业分包，无需提供分包意向协议；

4.本项目的特定资格要求：

无。

有特定资格要求： ，该特定条件的法律法规依据： 。

5.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，不得参加同一合同项下的政府采购活动；为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后不得再参加该采购项目的其他采购活动。

**三、获取招标文件**

**时间：**/至2024年5月16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/在线申请获取采购文件（进入“项目采购”应用，在获取采购文件菜单中选择项目，申请获取采购文件）。

**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：** 2024年5月16日10点30分00秒 （北京时间）

**投标地点（网址）：**政采云平台（https://www.zcygov.cn/）

**开标时间：**2024年5月16日10点30分00秒

**开标地点（网址）：**政采云平台（https://www.zcygov.cn/）

**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.《浙江省财政厅关于进一步发挥政府采购政策功能全力推动经济稳进提质的通知》 （浙财采监（2022）3号）、《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号））、《浙江省财政厅关于进一步加大政府采购支持中小企业力度助力扎实稳住经济的通知》 （浙财采监（2022）8号）已分别于2022年1月29日、2022年2月1日和2022年7月1日开始实施，此前有关规定与上述文件内容不一致的，按上述文件要求执行。

2.根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表:鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

3.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。

4.其他事项：（1）需要落实的政府采购政策：包括节约资源、保护环境、支持创新、促进中小企业发展等。详见招标文件的第二部分总则。（2）电子招投标的说明：①电子招投标：本项目以数据电文形式，依托“政府采购云平台（www.zcygov.cn）”进行招投标活动，不接受纸质投标文件；②投标准备：注册账号--点击“商家入驻”，进行政府采购供应商资料填写；申领CA数字证书---申领流程详见“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”；安装“政采云电子交易客户端”----前往“浙江政府采购网-下载专区-电子交易客户端”进行下载并安装；③招标文件的获取：使用账号登录或者使用CA登录政采云平台；进入“项目采购”应用，在获取采购文件菜单中选择项目，获取招标文件；④投标文件的制作：在“政采云电子交易客户端”中完成“填写基本信息”、“导入投标文件”、“标书关联”、“标书检查”、“电子签名”、“生成电子标书”等操作；⑤采购人、采购机构将依托政采云平台完成本项目的电子交易活动，平台不接受未按上述方式获取招标文件的供应商进行投标活动； ⑥对未按上述方式获取招标文件的供应商对该文件提出的质疑，采购人或采购代理机构将不予处理；⑦不提供招标文件纸质版；⑧投标文件的传输递交：投标人在投标截止时间前将加密的投标文件上传至政府采购云平台，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。备份投标文件的制作、存储、密封详见招标文件第二部分第15点—“备份投标文件”；⑨投标文件的解密：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。通过“政府采购云平台”上传递交的投标文件无法按时解密，投标供应商递交了备份投标文件的，以备份投标文件为依据，否则视为投标文件撤回。通过“政府采购云平台”上传递交的投标文件已按时解密的，备份投标文件自动失效。投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效；⑩具体操作指南：详见政采云平台“服务中心-帮助文档-项目采购-操作流程-电子招投标-政府采购项目电子交易管理操作指南-供应商”。（3）招标文件公告期限与招标公告的公告期限一致。

**七、对本次采购提出询问、质疑、投诉，请按以下方式联系**

1.采购人信息

名 称：杭州市数据资源管理局

地 址：杭州市上城区解放东路18号

项目联系人（询问）：王先生

项目联系方式（询问）：0571-85250507

质疑联系人：张先生

质疑联系方式：0571-85250404（请通过以下路径在线提起质疑：政采云-项目采购-询问质疑投诉-质疑列表）

2.采购代理机构信息

名 称：杭州市公共资源交易中心

地 址：杭州市上城区之江路925号

传 真： /

项目联系人（询问）： 潘工、张工

项目联系方式（询问）：0571-85085361、85085067

质疑联系人： 谢栋华

质疑联系方式：0571-85085477（请通过以下路径在线提起质疑：政采云-项目采购-询问质疑投诉-质疑列表）

3.同级政府采购监督管理部门

名 称：杭州市财政局政府采购监管处 /浙江省政府采购行政裁决服务中心（杭州）

地 址：杭州市上城区四季青街道新业路市民之家G03办公室

传 真： /

联系人 ：朱女士、王女士

监督投诉电话： 0571-85252453

政策咨询：陈先生、厉先生，0571-89580460、89580456

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95763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** | **本项目的特别规定** |
| --- | --- | --- |
| 1 | **项目属性** | 服务类。 |
| 2 | **采购标的及其对应的中小企业划分标准所属行业** | （1）标的： 杭州市智慧电子政务外网（2024）项目 ，属于 软件和信息技术服务业 行业； |
| 3 | **是否允许采购进口产品** | 本项目不允许采购进口产品。  可以就 采购进口产品。优先采购向我国企业转让技术、与我国企业签订消化吸收再创新方案的供应商的进口产品，详见评分标准。 |
| 4 | **分包** | A同意将非主体、非关键性的 设备维保、部分运维人员 工作分包。  B不同意分包。  注：不得限制大中型企业向小微企业合理分包。 |
| 5 | **开标前答疑会或现场考察** | A不组织。  B组织，时间： ,地点： ，联系人： ，联系方式： 。 |
| 6 | **样品提供** | A不要求提供。  B要求提供（未提供样品或提供样品不满足采购需求实质性条件的供应商，投标无效）：  （1）样品： ；  （2）样品制作的标准和要求： ；  （3）样品的评审方法以及评审标准：  样品分未超过价格分的50%；  样品分超过价格分的50%，理由 ；  详见招标文件第四部分评标办分法。  （4）是否需要随样品提交检测报告：否；是，检测机构的要求： ；检测内容： 。  （5）提供样品的时间： ；地点： ；联系人： ，联系电话： 。请投标人在上述时间内提供样品并按规定位置安装完毕。超过截止时间的，采购人或采购代理机构将不予接收，并将清场并封闭样品现场。  (6)采购活动结束后，对于未中标人提供的样品，采购人、采购机构将通知未中标人在规定的时间内取回，逾期未取回的，采购人、采购机构不负保管义务；对于中标人提供的样品，采购人将进行保管、封存，并作为履约验收的参考。  （7）制作、运输、安装和保管样品所发生的一切费用由投标人自理。 |
| 7 | **方案讲解演示** | A不组织。  B组织。  （1）在评标时安排每个投标人进行方案讲解演示。每个投标人时间不超过20分钟，讲解次序以投标文件解密时间先后次序为准，讲解演示人员不超过3人。讲解演示结束后按要求解答评标委员会提问。  （2）方案讲解演示可选择以下其中一种方式：  方式一：政采云平台在线讲解演示。政采云平台在线讲解需投标人根据政采云平台操作要求做好准备工作，提前完善软硬件配置环境。  方式二：交易中心现场讲解演示。现场讲解地点为杭州市公共资源交易中心4楼答疑室（讲标室），讲解演示所用电脑等设备由投标人自备。现场讲解演示人员进场时提供讲解人员名单（加盖公章或授权代表签名）及身份证明，否则不得讲解演示。  注：因投标人自身原因导致无法演示或者演示效果不理想的，责任自负。因平台原因导致本项目方案讲解演示环节无法顺利开展，按照《浙江省政府采购项目电子交易管理暂行办法》相关规定执行。 |
| 8 | **投标人应当提供的资格、资信证明文件** | （1）资格证明文件：见招标文件第二部分11.1。  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，投标无效。 |
| （2）资信证明文件：根据招标文件第四部分评标标准提供。 |
| 9 | **节能产品、环境标志产品政府优先采购或强制采购** | 依据国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，对获得证书的产品实施政府优先采购或强制采购；其中，对产品名称XXX实施政府优先采购，详见评分标准；▲对产品名称XXX实施政府强制采购，**投标人就相应的投标产品未提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的，投标无效**。  依据国家确定的认证机构出具的、处于有效期之内的环境标志产品认证证书，对获得证书的产品名称XXX实施政府优先采购，详见评分标准。  无。 |
| 10 | **报价要求** | 有关本项目实施所需的所有费用（含税费）均计入报价。**投标文件开标一览表（报价表）是报价的唯一载体，如投标人在政府采购云平台填写的投标报价与投标文件报价文件中开标一览表（报价表）不一致的，以报价文件中开标一览表（报价表）为准。**投标文件中价格全部采用人民币报价。招标文件未列明，而投标人认为必需的费用也需列入报价。**提醒：验收时检测费用由采购人承担，不包含在投标总价中。**  **投标报价出现下列情形的，投标无效：**  **投标文件出现不是唯一的、有选择性投标报价的；**  **投标报价超过招标文件中规定的预算金额或者最高限价的;**  **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，未能按要求提供书面说明或者提交相关证明材料证明其报价合理性的;**  **投标人对根据修正原则修正后的报价不确认的。** |
| 11 | **中小企业信用融资** | 供应商中标后也可在“政采云”平台申请政采贷：操作路径：登录政采云平台 - 金融服务中心 -【融资服务】，可在热门申请中选择产品直接申请，也可点击云智贷匹配适合产品进行申请，或者在可申请项目中根据该项目进行申请。 |
| 12 | **备份投标文件送达地点和签收人员** | 备份投标文件送达地点：杭州市之江路925号临江金座2号楼1010室（杭州市公共资源交易中心政府采购处） ；备份投标文件签收人员联系电话： 0571-87008103。**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。** |
| 13 | **特别说明** | 联合体投标的，联合体各方分别提供与联合体协议中规定的分工内容相应的业绩证明材料，业绩数量以提供材料较少的一方为准。招标文件第四部分评分标准有其他规定的，从其规定。 |
| 联合体投标的，联合体各方均需按招标文件第四部分评标标准要求提供资信证明文件，否则视为不符合相关要求。招标文件第四部分评分标准有其他规定的，从其规定。  联合体投标的，联合体中有一方或者联合体成员根据分工按招标文件第四部分评标标准要求提供资信证明文件的，视为符合了相关要求。招标文件第四部分评分标准有其他规定的，从其规定。 |
| 招标文件第四部分评审因素对应的要求及第五部分采购合同的内容视为采购需求的一部分。 |
| 本项目评审报告推荐的中标候选人数量： 1 。 |

**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“电子签名”系指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据；“公章”系指单位法定名称章。因特殊原因需要使用冠以法定名称的业务专用章的，投标时须提供《业务专用章使用说明函》（附件4）。

2.6“电子交易平台”是指本项目政府采购活动所依托的政府采购云平台（https://www.zcygov.cn/）。

2.7 “▲” 系指实质性要求条款，“” 系指适用本项目的要求，“” 系指不适用本项目的要求。

**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）；优先采购向我国企业转让技术、与我国企业签订消化吸收再创新方案的供应商的进口产品。

3.2 支持绿色发展

3.2.1采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构将依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。投标人须按招标文件要求提供相关产品认证证书。**▲采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人相应的投标产品未获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的，投标无效。**

3.2.2 修缮、装修类项目采购建材的，采购人应将绿色建筑和绿色建材性能、指标等作为实质性条件纳入招标文件和合同。

3.2.3为助力打好污染防治攻坚战，推广使用绿色包装，政府采购货物、工程和服务项目中涉及商品包装和快递包装的，供应商提供产品及相关快递服务的具体包装要求要参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》。优先采购绿色包装产品、绿色物流配送服务以及循环利用产品。

3.3支持中小企业发展

3.3.1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。

3.3.2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：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。

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。

3.3.3对于未预留份额专门面向中小企业的政府采购服务项目，以及预留份额政府采购服务项目中的非预留部分标项，对小型和微型企业的投标报价给予10%-20%（招标文件第四部分评标办法明确具体的扣除比例，未明确的，给予20%的扣除）的扣除，用扣除后的价格参与评审。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政府采购服务项目，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，对联合体或者大中型企业的报价给予4%-6%（招标文件第四部分评标办法明确具体的扣除比例，未明确的，给予6%的扣除）的扣除，用扣除后的价格参加评审。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。

3.3.4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；

3.3.5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。

3.3.6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》，投标人提供的《中小企业声明函》与实际情况不符的，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

3.3.7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。

3.4支持创新发展

3.4.1 采购人优先采购被认定为首台套产品和“制造精品”的自主创新产品。

3.4.2首台套产品被纳入《首台套产品推广应用指导目录》之日起3年内，以及产品核心技术高于国内领先水平，并具有明晰自主知识产权的“制造精品”产品，自认定之日起2年内视同已具备相应销售业绩，参加政府采购活动时业绩分值为满分。

3.4.3 采购人应当贯彻落实知识产权保护相关法律法规，应当采购使用正版软件。3.5平等对待内外资企业和符合条件的破产重整企业

平等对待内外资企业和符合条件的破产重整企业，切实保障企业公平竞争，平等维护企业的合法利益。**4. 询问、质疑、投诉、补偿救济**

4.1在线询问、质疑、投诉。根据《浙江省财政厅关于进一步促进政府采购公平竞争打造最优营商环境的通知》（浙财采监（2021）22号）文件关于“健全行政裁决机制”要求，鼓励供应商在线提起询问，路径为：政采云-项目采购-询问质疑投诉-询问列表；鼓励供应商在线提起质疑，路径为：政采云-项目采购-询问质疑投诉-质疑列表。质疑供应商对在线质疑答复不满意的，可在线提起投诉，路径为：浙江政府服务网-政府采购投诉处理-在线办理。

4.2供应商询问

供应商对政府采购活动事项有疑问的，可以提出询问，采购人或者采购代理机构应当在3个工作日内对供应商依法提出的询问作出答复，但答复的内容不得涉及商业秘密。供应商提出的询问超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知供应商向采购人提出。

4.3供应商质疑

4.3.1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。

4.3.2供应商认为招标文件、采购过程和中标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：

4.3.2.1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。

4.3.2.2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。4.3.2.3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。

4.3.3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：

　　4.3.3.1供应商的姓名或者名称、地址、邮编、联系人及联系电话；

　　4.3.3.2质疑项目的名称、编号；

　　4.3.3.3具体、明确的质疑事项和与质疑事项相关的请求；

　　4.3.3.4事实依据；

　　4.3.3.5必要的法律依据；

4.3.3.6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。

4.3.4对同一采购程序环节的质疑，供应商须在法定质疑期内一次性提出。

4.3.5采购人或者采购机构应当根据《杭州市集中采购委托协议》的约定，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。根据《杭州市财政局关于进一步加强政府采购信息公开优化营商环境的通知》（杭财采监〔2021〕17号）,采购人或者采购机构在质疑回复后5个工作日内，在浙江政府采购网的“其他公告”栏目公开质疑答复，答复内容应当完整。质疑函作为附件上传。

根据采购人与采购机构签订的《杭州市集中采购委托协议》的约定，质疑答复责任主体如下：

**质疑答复责任主体一览表**

|  |  |  |
| --- | --- | --- |
| **质疑内容** | | **质疑答复责任主体** |
| 对采购文件提出质疑 | 对采购文件中“申请人的资格要求”、“采购需求”、“评审办法”、“采购合同的主要条款”、“采购文件前附表内容”、“报价内容”的质疑 | 采购人 |
| 对采购文件中其他内容提出的质疑 | 采购机构 |
| 对采购过程、采购结果提出质疑 | 对“现场考察、答疑会”、 “甲方负责接收和保存的样品” 、“资格审查”等由采购人负责组织的环节的质疑 | 采购人 |
| 对采购过程、采购结果其他环节的质疑 | 采购机构 |

4.3.6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。

4.4供应商投诉

4.4.1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。

4.4.2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。

4.4.3供应商投诉应当有明确的请求和必要的证明材料。

4.4.4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。

4.4.5浙江省本级、杭州市本级、拱墅区、富阳区政府采购项目投诉材料可寄送浙江省政府采购行政裁决服务中心（杭州），地址：杭州市上城区四季青街道新业路市民之家G03办公室，收件人：朱女士，电话：0571-85252453。

投诉书范本及制作说明详见附件3。

4.5 补偿救济

采购人（行政机关）因政策变化、规划调整而不履行政府采购合同的，供应商可依据《杭州市涉企补偿救济实施办法（试行）》向采购人（行政机关）提起补偿申请。

**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：

5.1.1招标公告；

5.1.2投标人须知；

5.1.3采购需求；

5.1.4评标办法；

5.1.5拟签订的合同文本；

5.1.6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的内容为招标文件的组成部分。

**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。

6.2 采购机构对招标文件进行澄清或修改的，将同时通过电子交易平台通知已获取招标文件的潜在投标人。依法应当公告的，将按规定公告，同时视情况延长投标截止时间和开标时间。该澄清或者修改的内容为招标文件的组成部分。

**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、方式及招标文件售价。

**8.开标前答疑会或现场考察**

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，潜在投标人按第二部分投标人须知前附表的规定参加现场考察或者开标前答疑会。

**9.投标保证金**

本项目不需缴纳投标保证金。

**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**

11.1**资格文件**：

11.1.1符合参加政府采购活动应当具备的一般条件的承诺函；

11.1.2联合协议（如果有)；

11.1.3落实政府采购政策需满足的资格要求（如果有)；

11.1.4本项目的特定资格要求（如果有)。

11.2 商务技术文件：

11.2.1投标函；

11.2.2授权委托书或法定代表人（单位负责人、自然人本人）身份证明；

11.2.3分包意向协议（如果有)；

11.2.4符合性审查资料；

11.2.5评标标准相应的商务技术资料；

11.2.6投标标的清单；

11.2.7商务技术偏离表；

11.2.8政府采购供应商廉洁自律承诺书；

11.3**报价文件：**

11.3.1开标一览表（报价表）；

11.3.2 报价情况说明（如供应商报价低于项目预算50%的，应当提交本文档，详细阐述不影响产品质量或者诚信履约的具体原因）；

11.3.3中小企业声明函。

**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。**

**投标人应对投标文件中材料的真实性、合法性负责。**

**12. 投标文件的编制**

12.1投标文件分为资格文件、商务技术文件、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名。

13.3招标文件对投标文件签署、盖章的要求适用于电子签名。

**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。供应商撤回投标不得损害国家利益、社会公共利益、采购人利益、代理机构利益、其他供应商利益，否则，供应商撤销（撤回）投标无效。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采购人、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**

15.1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。**

15.2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(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协议中约定的牵头人的名称)。**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。**

15.3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。

15.4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招标文件第二部分投标人须知前附表规定的备份投标文件送达地点；送达时间以签收人签收时间为准。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。

**15.5投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效。**

**16.投标文件的无效处理**

有招标文件第四部分4.2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，采购机构可以以书面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。

17.4在投标截止时间起至投标有效期届满，供应商投标文件不可撤销。

**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**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。**

**19、资格审查**

19.1开标后，采购人将依据法律法规和招标文件的规定，对投标人的资格进行审查。

19.2投标人未按照招标文件要求提供与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。

19.3对未通过资格审查的投标人，告知其未通过的原因。

19.4合格投标人不足3家的，不再评标。

19.5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，并且获得总机构授权或能够提供房产权证或其他有效财产证明材料，证明其具备实际承担责任的能力和法定的缔结合同能力，可以允许其独立参加政府采购活动。

**20、信用信息查询**

20.1信用信息查询渠道及截止时间：采购机构将在资格审查时通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道查询投标人接受资格审查时的信用记录。

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采购文件一起存档。

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.** 评标委员会将根据招标文件和有关规定，履行评标工作职责，并按照评标方法及评分标准，全面衡量各投标人对招标文件的响应情况。对实质上响应招标文件的投标人，按照评审因素的量化指标排出推荐中标的投标人的先后顺序，并按顺序提出授标建议。**详见招标文件第四部分评标办法。**

**六、定 标**

**22. 确定中标供应商**

政府采购项目实行全流程电子化，评审报告送交、采购结果确定和结果公告均在线完成。为进一步提升采购结果确定效率，采购代理机构应当依法及时将评审报告在线送交采购人。采购单位应当自收到评审报告之日起2个工作日内在线确定中标或者成交供应商，为提高政府采购效率，鼓励在收到评审报告当天在线确定中标或者成交供应商。在采购结果确认环节，中标候选人撤销投标文件不能成为采购人不确认采购结果的正当理由。中标、成交通知书和中标、成交结果公告应当在规定时间内同时发出。

**23. 中标通知与中标结果公告**

23.1自中标人确定之日起2个工作日内，采购机构通过电子交易平台向中标人发出中标通知书，同时编制发布采购结果公告。采购机构也可以以纸质形式进行中标通知。

23.2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，开标记录、资格审查情况、评审专家抽取规则、符合性审查情况、未中标情况说明、中标公告期限以及评审专家名单、评分汇总及明细。

23.3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通过电子交易平台在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，并在签订之日起2个工作日内将政府采购合同在浙江政府采购网上公告。鼓励有条件的采购人视情缩减采购合同签订时限，提高采购效率，杜绝“冷、硬、横、推”等不当行为。除不可抗力等特殊情况外，原则上应当在中标通知书发出之日起10个工作日内，与中标供应商按照采购文件确定的事项签订政府采购合同。

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。

25.5采购合同由采购人与中标供应商根据招标文件、投标文件等内容通过政府采购电子交易平台在线签订，自动备案。

**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1%。鼓励和支持供应商以银行、保险公司出具的保函形式提供履约保证金。采购人不得拒收履约保函，项目验收结束后应及时退还，延迟退还的，应当按照合同约定和法律规定承担相应的赔偿责任。

## 供应商可登录政采云平台-【金融服务】—【我的项目】—【已备案合同】以保函形式提供：1、供应商在合同列表选择需要投保的合同，点击[保函推荐]。2、在弹框里查看推荐的保函产品，供应商自行选择保函产品，点击[立即申请]。3、在弹框里填写保函申请信息。具体步骤：选择产品—填写供应商信息—选择中标项目—确认信息—等待保险/保函受理—确认保单—支付保费—成功出单。政采云金融专线400-903-9583。

## **27.预付款**

采购单位应当在政府采购合同中约定预付款，对中小企业合同预付款比例原则上不低于合同金额的40％，不高于合同金额的70%；项目分年安排预算的，每年预付款比例不低于项目年度计划支付资金额的40％，不高于合同金额的70%；采购项目实施以人工投入为主的，可适当降低预付款比例，但不得低于20%。对供应商为大型企业的项目或者以人工投入为主且实行按月定期结算支付款项的项目，预付款可低于上述比例或者不约定预付款。在签订合同时，供应商明确表示无需预付款或者主动要求降低预付款比例的，采购单位可不适用前述规定。采购单位根据项目特点、供应商诚信等因素，可以要求供应商提交银行、保险公司等金融机构出具的预付款保函或其他担保措施。政府采购预付款应在合同生效以及具备实施条件后5个工作日内支付。政府采购工程以及与工程建设有关的货物、服务，采用招标方式采购的，预付款从其相关规定。供应商可登录政采云前台大厅选择金融服务 - 【保函保险服务】出具预付款保函，具体步骤：选择产品—填写供应商信息—选择中标项目—确认信息—等待保险/保函受理—确认保单—支付保费—成功出单。政采云金融专线400-903-9583。

**八、电子交易活动的中止**

2**8. 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：

28.1电子交易平台发生故障而无法登录访问的；

28.2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；

28.3电子交易平台发现严重安全漏洞，有潜在泄密危险的；

28.4病毒发作导致不能进行正常操作的；

28.5其他无法保证电子交易的公平、公正和安全的情况。

29.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，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。

**九、验收**

**30.验收**

30.1采购人应当根据采购项目的具体情况，自行组织项目验收或者委托采购代理机构验收。采购人组织对供应商履约的验收。大型或者复杂的政府采购项目，应当邀请国家认可的质量检测机构参加验收工作。验收方成员应当在验收书上签字，并承担相应的法律责任。如果发现与合同中要求不符，供应商须承担由此发生的一切损失和费用，并接受相应的处理。

30.2采购人可以邀请参加本项目的其他投标人或者第三方机构参与验收。参与验收的投标人或者第三方机构的意见作为验收书的参考资料一并存档。

30.3严格按照采购合同开展履约验收。采购人成立验收小组，按照采购合同的约定对供应商履约情况进行验收。验收时，按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后，应当出具验收书，列明各项标准的验收情况及项目总体评价，由验收双方共同签署。验收结果与采购合同约定的资金支付及履约保证金返还条件挂钩。履约验收的各项资料应当存档备查。

30.4验收合格的项目，采购人将根据采购合同的约定及时向供应商支付采购资金、退还履约保证金。验收不合格的项目，采购人将依法及时处理。采购合同的履行、违约责任和解决争议的方式等适用《中华人民共和国民法典》。供应商在履约过程中有政府采购法律法规规定的违法违规情形的，采购人应当及时报告本级财政部门。

30.5 对于满足合同约定的采购资金支付条件的，供应商可通过政采云平台提起在线支付申请、查询支付结果，路径为政采云-我的工作台-合同管理-支付管理。对于供应商提起在线支付申请的，采购人应当按规定做好审核并完成支付。

**第三部分 采购需求**

1. **项目背景**

2006年6月根据《浙江省人民政府办公厅关于建设省电子政务网络平台的通知》（浙政办函〔2003〕88号）和《浙江省电子政务网络技术规范》的要求，对杭州市电子政务网络进行建设改造。

市电子政务外网网络包括核心层、汇聚层、客户端、接入层、安全系统等各类网络设备，负责全市电子政务外网各类业务系统的正常运行。

2017年，《浙江省人民政府办公厅关于开展政务专网整合和加强政务网外围安全防护工作的通知》浙政办发【2017】140号，杭州市数据局积极推进专网整合、互联网出口整合。

至今，电子政务网整合了现有多张专网，包括交通专网、审计专网等；整合了大部分局委办的自有互联网出口，政务网底层网络数据交互流量、出口互联网流量有了巨大的增长。

根据国办电政函〔2018〕70号中关于推进国家电子政务外网互联网协议第六版（IPV6）改造工作的通知要求，2020年底前，完成市地级政务外网IPV6改造，全面支持市地级以上政务部门IPV6门户网站部署；根据工业和信息化部关于贯彻落实《推进互联网协议第六版（IPv6）规模部署行动计划》的通知（工信部通信〔2018〕77号），工信部开展2020年IPv6端到端贯通能力提升专项行动，特别提出要优化提升IPv6网络接入能力，全面扩大数据中心IPv6覆盖范围，到2020年底IPv6活跃连接数达到11.5亿。

杭州市电子政务网核心网已支持IPV4/IPV6双栈，但考虑到未来3年的发展需求，电子政务网作为IPV6的重要组成部分，也对整个电子政务网的基础性能提出了更高的要求。

根据国办电政函〔2018〕70号中关于推进国家电子政务外网互联网协议第六版（IPV6）改造工作的通知要求，2020年底前，完成市地级政务外网IPV6改造，全面支持市地级以上政务部门IPV6门户网站部署。

随着数字化转型步入深水区，大数据、云计算、物联网等基础应用持续深化，数据泄露、高危漏洞、网络攻击以及相关的智能犯罪等网络安全问题也呈现出新变化，严重危害国家关键基础设施安全、挑战公民隐私安全甚至危及社会稳定。

1. **项目内容**

通过本次项目服务提高电子政务外网基础承载能力，预计目标为解决现有网络系统中存在的问题隐患，同时提升电子政务外网的整体性能、安全性、可管理性等，为杭州市打造数字型政府、争做数字经济第一城、实现最多跑一次等目标提供更为稳定、可靠、优质的基础网络平台。

分项目标如下：

(一)出口带宽续费为提升整体电子政务外网性能提供坚实的链路基础，也很好的满足了政策要求。

(二)政务网部分核心设备的服务进一步提高了杭州市电子政务外网承载能力。

(三)电子政务外网整体安全系统服务进一步、适应更加复杂多变的网络环境。

(四)原有政务网设备的质保服务进一步增加了电子政务外网的可靠性、可运营、可管理。

(五)充分考虑到目前替换闲置的设备和板卡，保护现有投资。

(六)根据业务需求，灵活扩充带宽，实现资金节约，分布投入。

1. **采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范等**

* 《国家电子政务工程建设项目管理暂行办法》
* 《国家电子政务标准化指南》，国信办和国家标准委员会
* 《政务信息资源交换体系技术标准》（GB/T21062-2007）
* 《杭州市信息化推进法律法规汇编》
* 《关于印发二○一四年杭州市政府投资信息化项目建设指导意见的通知》(杭信〔2013〕3号)
* 《“互联网+政务服务”技术体系建设指南》

1. **目标**

本次项目目标是完成杭州市电子政务外网核心承载网服务能力的提升改造。属于信息化基础设施，此承载网将服务于全市电子政务网接入单位及相关机构。本项目为采购服务，周期为1年。

服务内容分为以下3块内容：线路资源租赁服务，设备租赁服务，设备维保服务。

1. **原则**

杭州市电子政务网作为全市电子政府开展的基础，其重要性不言而喻，目标是实现一个完整统一、组网灵活、易扩充的网络平台，满足传送语音、文字、数据、图像、VPN等各类综和信息业务。

总的来说，设备选型要技术先进，能适应未来发展，具有灵活方便的业务扩展能力和充分完备的接入能力，设备及其软件具有可持续发展的平滑升级性；在技术选择上综合考虑先进性、成熟性及良好的性价比，以网络的可扩展性和可管理性为基础，统一规划，分步实施。

**开放性**：为了保证系统的持续发展和系统不同设备的互联互通，所采用的网络技术应符合国际标准的通信协议、标准化接口和我国的技术规范，支持良好的维护、测量及管理手段，提供网络统一实时监控的信息处理功能，实现网络的统一管理。

**可运营性**：实现IP网络的目的就是能向大量用户提供良好的业务管理能力，支持对宽带用户的接入管理、身份认证、地址管理和服务质量（QoS），并针对不同的业务提供灵活的计费方式，确保网络的可运营性。

**可管理性**：IP网络是分层的网络结构，需要统一的网络业务调度和管理，降低网络运营成本。

**可扩充性**：用户数量和宽带业务种类发展有着不确定性。随着业务需求的不断变化，要求IP运营网络实现成完整统一、组网灵活、易扩充的弹性网络平台。

**安全可靠性**：网络的设计要充分考虑到其稳定性，支持网络节点的备份和线路保护，提供网络安全防范措施。

1. **项目服务清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 要求 | | 数量 | 单位 | 服务期 |
| 一、线路资源租赁服务 | | | |  |  |  |
| 1 | 互联网出口带宽租用服务 | 互联网出口带宽不少于8.3G | | 1 | / | 1年 |
| 2 | 政务外网线路租赁服务 | 包含政务网VPN100M、政务网VPN500M、政务网VPN1000M、政务网裸光纤、光纤专线10M、光纤专线50M、公共安全区接入线路条等类型 | | 1 | / | 1年 |
| 3 | 统一运维服务 | 现场驻场服务共5人（4名技术驻场人员，对市民中心政务外网有线、无线网进行日常运维；1名安全技术驻场人员，在市民中心政务外网网络稳定运行的基础上，负责基础网络安全运维）。驻场人员具体工作包括政务外网网络服务开通，有线、无线网运行保障，网络故障修复，网络应急事件响应，重大任务保障等，还需要定期对网络机房及设备进行巡检巡查（按季度完成政务网定期巡检服务并提供巡检报告），平台维护，省市对接等以保证市民中心政务外网的稳定运行。  另外再提供一人为因重点保障按业主需要随时驻场完成省市数据对接采集等维护工作。 | | 1 | / | 1年 |
| 二、设备租赁服务 | | | |  |  |  |
| 1、网络、安全设备租赁服务 | | | |  |  |  |
| 1 | 出口负载均衡设备 | 性能不低于：4层吞吐量：65Gbps，并发连接数：41000000，4层新建连接数CPS：750000，7层新建连接数RPS：280000，7层新建连接数RPS：610000。硬盘容量不低于：80GSSD，电源：冗余电源，接口不少于：4千兆电口+8千兆光口SFP+8万兆光口SFP+ | | 2 | 台 | 1年 |
| 2 | 出口路由设备 | 性能不低于：每台配置不少于24万兆端口、20千兆端口；双引擎、双电源、独立交换网板；含配套10KM万兆单模光模块 | | 2 | 台 | 1年 |
| 3 | 出口上网行为管理设备 | 性能不低于：吞吐量：不小于25Gb，支持用户数不小于：100000；硬盘容量不小于：SATA1T+64GSSD，电源：冗余电源，接口不少于：4千兆电口+4千兆光口SFP+8万兆光口SFP+ | | 2 | 台 | 1年 |
| 4 | 市民中心核心网镜像流量设备 | 性能不低于：48万兆光口,4个40G光口，含配套10KM万兆单模光模块 | | 2 | 台 | 1年 |
| 5 | 政务云出口交换机设备 | 性能不低于：24万兆光口汇聚交换机，含配套10KM万兆单模光模块 | | 2 | 台 | 1年 |
| 6 | 政务网核心路由器（P设备）冷备设备 | 原有电子政务网核心路由器冷备 | | 1 | 台 | 1年 |
| 7 | 城域网汇聚交换机（涉及4个汇聚机房、热备）设备 | 性能不低于：24万兆光口汇聚交换机，含配套10KM万兆单模光模块 | | 8 | 台 | 1年 |
| 8 | 城域网PE交换机板卡 | 24端口万兆以太网光接口和24端口千兆以太网光接口板(X6S,SFP+)满配万兆单模光模块及千兆单模光模块 | | 4 | 块 | 1年 |
| 9 | 市民中心AC设备 | 无线控制器 | | 2 | 台 | 1年 |
| 10 | 市民中心吸顶AP设备 | 吸顶AP | | 134 | 台 | 1年 |
| 11 | 市民中心面板AP设备 | 面板AP | | 243 | 台 | 1年 |
| 12 | 电子政务外网专业DNS服务设备 | DNSQPS指标不低于10万/秒 | | 2 | 台 | 1年 |
| 13 | 电子政务外网专业DHCP服务设备 | DHCPLPS指标不低于2000/秒 | | 2 | 台 | 1年 |
| 14 | 短信服务 | 一年不超过20W条短信 | | 1 | 项 | 1年 |
| 15 | 公共接入区防火墙设备 | 网络处理能力60Gbps，并发连接≥1200万，每秒新建连接45万/秒。包含应用控制、病毒防护、入侵防御特征库服务 | | 1 | 台 | 1年 |
| 16 | 公共接入区数据安全交换系统设备 | 交换能力：≥8Gbps；并发会话：30000个 | | 1 | 套 |
| 17 | 公共接入区视频安全交换系统设备 | 支持2000路D1图象（2Mbps）或≥1000路高清（4Mbps） | | 1 | 套 |
| 18 | 机房优化服务 | 将机房中政务云节点搬迁至运营商机房，并且对机房进行优化，满足实际要求 | | 1 | 项 | 1年 |
| 19 | 一键封堵 | 实现和安全管控平台对接，对政务外网实现一键封堵 | | 1 | 项 | 1年 |
| 实现市政务外网基础网络边界设备的一键封堵，做到7\*24小时不间断封堵，支持对接第三方平台 | |
| 20 | 省市边界防火墙 | 省市边界防火墙，含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN功能；多核AMP+架构，网络层吞吐量≥60G，并发连接≥850万，每秒新建连接数≥60万，标准2U机箱，冗余电源， 标准配置1个Console口 、1个HA接口，1个MGT接口，4个万兆光口，支持2路万兆光口bypass；支持3个扩展插槽；支持液晶屏。含应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。须支持MPLS流量透传，对带有MPLS数据包流量进行封装/解封装，对数据包内容进行安全检查和分析，进而按照既定安全策略，进行转发和抛弃处理，对于转发的数据包还原标记并进行封装转发。支持针对MPLS流量的安全审查，包括漏洞防护、防病毒、流量控制、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能 | | 2 | 台 | 1年 |
| 21 | 运维区防火墙 | 运维区防火墙，性能不低于：网络层吞吐量：15G，应用层吞吐量：8G，防病毒吞吐量：1G，IPS吞吐量：1G，全威胁吞吐量：800M，并发连接数：200万，HTTP新建连接数：9万 | | 1 | 台 | 1年 |
| 22 | 电子政务外网违规外联检测设备 | 部署VPN2、VPN3各一台 | | 2 | 台 | 1年 |
| 23 | 电子政务网态势感知设备 | 性能不低于：存储容量：32T，在带宽性能1Gbps时存储时长：1800天/1Gbps | | 1 | 台 | 1年 |
| 24 | 市民中心数据流量探针设备 | 性能不低于：吞吐性能：≤3Gbps，内存不小于：32G，硬盘容量不小于：1TBSATA，电源：冗余电源，接口不少于：6千兆电口+2万兆光口SFP+ | | 1 | 台 | 1年 |
| 25 | 电子政务外网VPN设备 | 性能不低于：最大理论加密流量（Mbps）：350，最大理论并发用户数：8000，IPSec加密最大流量（Mbps）：200，设备整机理论最大吞吐量：1.2Gbps，设备整机理论最大并发会话数：150W | | 1 | 台 | 1年 |
| 26 | 内网数据防护设备 | 网络吞吐量：1.2Gb，支持用户数：不少于1200 | | 1 | 台 | 1年 |
| 27 | 数据库审计设备 | 事件处理不小于18000条/秒 | | 1 | 台 | 1年 |
| 28 | 电子政务外网与政务云边界防护设备 | 性能不低于：吞吐量：不小于55G，接口：不少于6千兆电口+6万兆光口SFP+ | | 2 | 台 | 1年 |
| 29 | 市民中心局委办与电子政务外网边界防护设备 | 性能不低于：吞吐量：不小于50G，接口：不少于6千兆电口+6万兆光口SFP+ | | 2 | 台 | 1年 |
| 30 | 市民中心外围局委办（鸿鼎、劳技PE侧边界）边界防护设备 | 性能不低于：吞吐量：不小于50G，接口：不少于6千兆电口+6万兆光口SFP+ | | 2 | 台 | 1年 |
| 31 | 市民中心外围局委办（干休所、高银巷PE侧边界）边界防护设备 | 性能不低于：吞吐量：不小于55G，接口：不少于6千兆电口+6万兆光口SFP+ | | 2 | 台 | 1年 |
| 32 | 便携式CPE | 满足主要领导出差访问使用（含国内外1年流量） | | 1 | 套 | 1年 |
| 2、政务外网平台化运维能力租赁服务 | | | |  |  |  |
| 1 | 电子政务外网申请审批服务 | 政务外网VPN申请、墙口开通、有线、无线网络开通关闭，割接报备等流程 | | 1 | 项 | 1年 |
| 2 | 数据采集服务 | 政务外网设备和政务外网线路相关性能状态数据采集 | | 1 | 项 |
| 3 | 性能自动化告警服务 | 通过web界面中的告警首页，实时展示所有告警状态，告警节点、告警类型和告警内容，使网络管理员能清晰直观的知道网络中存在的问题，快速并准确的对应到告警设备，并对告警内容进行相对应的的处理 | | 1 | 项 |
| 4 | 数据展示服务 | 可视化呈现拓扑关系，展示对应设备的运行情况、实时展示所选线路信息，线路流量上限、线路实时流量等、按日、周、月统计设备运行情况、按分钟、日统计网络线路流量分布情况、可视化呈现封堵IP数量、黑名单数量、处理告警数量 | | 1 | 项 |
| 5 | 机房管理服务 | 对接机房感知设备，获得机房运行实时情况 | | 1 | 项 |
| 6 | 数据看板对接服务 | 和数字杭州数字数据看板对接，提供所需要的数据 | | 1 | 项 |
| 7 | 政务网线路精细化管理服务 | 对现在的政务外网线路，进行精细化管理，涵盖所有政务网情况，并且提供申请，变更，撤销，提醒等服务 | | 1 | 项 |
| 8 | DHCP数据清洗服务租用 | 存储，查询历史DHCP分配数据，为安全事件溯源提供数据支撑 | | 1 | 项 |
| 9 | 电子政务外网态势感知数据清洗服务租用 | 现有态势感知数据初步清洗后同步至市安全管控平台，为安全管控平台提供可用的网络区域的安全基础数据。 | | 1 | 项 |
| 10 | 骨干网全年无故障率指标服务租用 | 自动采集骨干链路数据形成全年无故障率指标 | | 1 | 项 |
| 3、市民中心机房设备租赁服务 | | | |  |  |  |
| 1 | 核心及汇聚机房、UPS机房（共8个机房）摄像机、录像机、电子门禁、防盗报警、静电地板吸水贴面、静电消除设备租赁服务 | 包含电子门禁 | | 7 | 套 | 1年 |
| 防盗报警 | | 7 | 套 |
| 静电地板吸水贴面 | | 7 | 套 |
| 静电消除设备 | | 7 | 套 |
| 摄像机 | | 18 | 台 |
| 硬盘录像机 | | 2 | 套 |
| UPS机房门禁 | | 1 | 套 |
| 2 | 机房网络柜精密空调租赁服务 | 适配现有核心机房模块化网络柜精密空调 | | 1 | 项 | 1年 |
| 3 | 机房网络柜蓄电池设备租赁服务 | 适配现有UPS电池柜，12V100AH铅酸蓄电池128节，蓄电池在环境温度20℃～25℃时的浮充运行寿命不低于12年，蓄电池采用全密封防泄漏结构，外壳无异常变形、裂纹及污迹，上盖及端子无损伤，正常工作时无酸雾逸出 | | 1 | 项 | 1年 |
| 4 | UPS机房消防钢瓶、气体灭火控制盘设备租赁服务 | UPS机房消防钢瓶、气体灭火控制盘设备租用服务，实现1个防火区的火灾报警和气体灭火控制 | | 1 | 项 | 1年 |
| 三、设备维保服务 | | | | | |  |
| 1 | 市民中心路由交换设备维保服务 | 核心交换机 | H3C S7608X | 2 | 台 | 原厂1年 |
| 核心路由器 | H3C SR-8803-X-S | 2 | 台 |
| 汇聚交换机 | H3CS7506E-NP4 | 4 | 台 |
| 华为S7706 | 4 | 台 |
| 准入认证 | H3C DR2000 | 1 | 套 |
| 2 | 核心PE设备 | 华为NE20E-S8 | 6 | 项 | 原厂1年 |
| P设备 | 华为S7706 | 6 | 项 |
| 汇聚交换机 | 华为 S5730-68C-SI-AC | 12 | 项 |
| 3 | 市民中心机房维保服务 | 机房配电系统 | | 1 | 项 | 原厂1年 |
| 汇聚机房气体灭火系统 | | 3 | 套 |
| 机房精密空调 | | 5 | 套 |
| 机房冷通道动环监控 | | 2 | 套 |
| 市民中心A座3楼机房UPS（主机） | | 2 | 台 |
| 汇聚机房(A、B、C、D、E、F)UPS维保 | | 6 | 项 |

1. **技术要求**
2. **线路资源租赁服务**

1.1 互联网出口带宽租赁服务

互联网出口带宽≥8.3G，适配现有杭州市电子政务外网。（为保障线路服务质量，须覆盖电信、移动、联通、华数线路）。

1.2 政务网链路租赁服务

政务网相关链路租用须不少于147条，政务网相关链路租用包含政务网VPN100M、政务网VPN500M、政务网VPN1000M、政务网裸光纤、光纤专线10M、光纤专线50M、公共安全区接入线路等类型。

|  |  |  |
| --- | --- | --- |
| 序号 | 类型 | 数量 |
| 1 | 政务网VPN100M | 108 |
| 2 | 政务网VPN500M | 9 |
| 3 | 政务网VPN1000M | 16 |
| 4 | 政务网裸光纤 | 7 |
| 5 | 光纤专线10M | 1 |
| 6 | 光纤专线50M | 1 |
| 7 | 公共安全区接入线路 | 5 |

备注：1、须包含本服务周期所必须的机房配套资源，如机柜、电源等。2、因链路使用的情况须按照实际需求进行规划和分配，故政务网链路租赁服务部分实际使用的链路规格、数量和费用应当以验收结果为准，且结算总价上限不得超过合同金额。3、乙方应保证选取使用的线路规格数量以采购人要求为准，并应接受采购人的监督检查。4、潜在投标商根据自有线路类型进行投标，但必须满足上述七种类型和数量要求。

|  |  |  |
| --- | --- | --- |
| 序号 | 服务内容 | 参数要求 |
| 1 | VPN100M | 带宽100M，应用MPLS多协议标记交换技术，结合传统路由技术的标记交换实现的IP VPN虚拟专用网络，支持后续业务扩展和带宽升级，所有设备和链路均专网专用；  （1） 支持多种接入方式，所有接入端口均采用电口或光口，接口类型具备可扩展性，与接入端进行匹配；  （2） 空闲状态链路延时≤10ms；  （3） 支持BGP或OSPF等动态路由模式，实现双链路动态路由冗余； |
| 2 | VPN500M | 带宽500M，应用MPLS多协议标记交换技术，结合传统路由技术的标记交换实现的IP VPN虚拟专用网络，支持后续业务扩展和带宽升级，所有设备和链路均专网专用；（1） 支持多种接入方式，所有接入端口均采用电口或光口，接口类型具备可扩展性，与接入端进行匹配。（2） 空闲状态链路延时≤10ms；（3） 支持BGP或OSPF等动态路由模式，实现双链路动态路由冗余； |
| 3 | VPN1000M | 带宽1000M，应用MPLS多协议标记交换技术，结合传统路由技术的标记交换实现的IP VPN虚拟专用网络，支持后续业务扩展和带宽升级，所有设备和链路均专网专用；（1） 支持多种接入方式，所有接入端口均采用电口或光口，接口类型具备可扩展性，与接入端进行匹配。（2） 空闲状态链路延时≤10ms；（3） 支持BGP或OSPF等动态路由模式，实现双链路动态路由冗余； |
| 4 | 政务网裸光纤 | 2芯裸光纤，提供光纤物理通道（不进行任何数据处理，不受链路数据带宽限制，满足业务传输效率和保密性的高的要求）； |
| 5 | 光纤专线10M | 10M光纤专线，支持为用户提供公网固定真实IP地址，用户访问互联网的同时可以方便地向互联网中的其他用户提供信息服务。支持带宽调整灵活，可依据用户需求由20M扩容至1000M，同时还可同时提供IPV4及IPV6地址服务； |
| 6 | 光纤专线50M | 50M光纤专线，支持为用户提供公网固定真实IP地址，用户访问互联网的同时可以方便地向互联网中的其他用户提供信息服务。支持带宽调整灵活，可依据用户需求由20M扩容至1000M，同时还可同时提供IPV4及IPV6地址服务; |
| 7 | 公共安全区接入链路 | 符合接入现有政务外网公共接入区要求。 |

1.3 统一运维服务

现场驻场服务共5人（4名网络技术驻场人员，对市民中心政务外网有线、无线网进行日常运维；1名安全技术驻场人员，在市民中心政务外网网络稳定运行的基础上，负责基础网络安全运维）。

另外再提供一人为因重点保障按业主需要随时驻场完成省市数据对接采集等维护工作。

具体工作包括政务外网网络服务开通，有线、无线网运行保障，网络故障修复，网络应急事件响应，重大任务保障等，还需要定期对网络机房及设备进行巡检巡查（按季度完成政务网定期巡检服务并提供巡检报告），平台维护，省市对接等以保证市民中心政务外网的稳定运行。

1. **设备租赁服务**
   1. 网络、安全设备租赁服务
      1. 出口负载均衡设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件参数 | 规格：2U，硬盘容量≥480GSSD，接口不少于4个千兆电口、8个千兆光口SFP、8个万兆光口SFP+；性能需满足：4层吞吐量≥65Gbps，并发连接数≥41000000。 |
| 设备部署 | 支持串接部署方式和旁路部署方式，支持三角传输模式。 |
| 多合一功能集成 | 提供针对多条出口线路的链路负载均衡功能，实现inbound和outbound流量的均衡调度，以及链路之间的冗余互备。 |
| 提供针对L4/L7内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求。 |
| 提供针对多站点业务发布的全局负载均衡功能，通过智能DNS等机制实现内外网用户对多个数据中心的最优接入路径选择。 |
| 可编程流量控制 | 通过某种编程语言（如lua）实现自定义的流量编排，对IP、TCP、UDP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。 |
| 链路负载均衡 | 支持静态IP和PPPOE两种线路接入方式，提供截图证明。 |
| 支持基于五元组条件（源IP地址，源端口，目的IP地址，目的端口，传输层协议号）来进行出站访问的流量调度分发。 |
| 支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。 |
| 内置国外域名地址库，国外域名不少于10万条，支持自动更新。可将访问国外域名的请求分发至指定线路，实现对国外域名访问的优化，提升用户体验。 |
| 内置完备的IP地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能。 |
| 服务器负载均衡 | 支持源IP、Cookie（插入/被动/改写）、HTTP-Header、SSLSessionID等多种会话保持机制，支持跨虚拟服务的会话保持。 |
| 支持用户自定义方式的健康检查，支持多种编程语言（如Python、Java等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。 |
| 高可用性 | 支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换；  支持基于链路流量进行有效性判断，能够在预设时间内进行主动探测。  支持高可用集群N+M部署方式，单集群支持16台设备，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换。 |
| 统一监控 | 支持联动现有的态势感知平台，同步链路信息日志、上报CPU、内存、网卡流量等信息，实现通过现有平台进行设备的集中管理、集中监控、多日志关联分析。 |
| 运维管理 | 支持全中文管理界面和HTTPS方式登录、用户角色管理、多级授权管理。 |
| 支持设置管理地址白名单列表，远程维护支持设置是否允许WAN/LAN。 |
| 支持将现有的负载均衡设备上导出的配置文件导入到所投设备中，导出格式支持json等，实现配置策略的同步 |
| 支持SNMPv1/v2c/v3，标准MIB库和自定义库，可接受第三方网管平台如zabbix的管理。 |

* + 1. 出口路由设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 体系架构 | 支持主控板、交换网板、业务板完全物理分离，主控板、交换网板、业务板分布在不同的物理槽位 |
| 为保证设备可靠性，设备的转发全部有交换网板完成，主控板不集成转发芯片 |
| 为保证可靠性，设备需支持板卡（含主控，线卡，交换网板等）直接热插拔，同时不需要插拔电源风扇等其他关键部件 |
| 支持独立交换网板≥4个 |
| ✰设备性能 | 交换容量≥115T，包转发率≥24000M |
| ✰业务槽位 | 整机框全物理尺寸的线卡槽位数≥8（非子卡槽位），不含主控、交换网板槽位 |
| 实配≥24个万兆光口（满配万兆10KM单模模块），≥20个千兆电口 |
| 支持子母卡架构，母卡和子卡均支持热插拔 |
| 单槽位转发性能 | 设备支持单槽单向最大带宽≥400Gbps |
| 电源系统 | 支持内置交流电源，不能配置外置交流电源，也不额外占用业务槽位 |
| 电源个数≥6个，电源系统支持N+M冗余，支持一体化供电方式，任意拔掉两个电源，设备能够正常运行 |
| 通风方式 | 支持前后通风 |
| 基本功能 | 支持PPP、MP、HDLC、ETHERNET等链路层协议 |
| MPLS标签数≥16K |
| 路由表项≥3M |
| 支持链路聚合（Linkaggregation），支持动态聚合、手工聚合、跨板聚合 |
| 支持不同带宽的链路捆绑功能 |
| 支持IPV4静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略，支持4MIPv4FIB |
| 支持IPv6静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+，支持2MIPv6FIB |
| 支持L2VPN、L3VPN、OptionA、B、C类跨域，支持16KVPN，支持4MVPN路由 |
| 组播VPN（MVPN） | 支持分布式MVPN功能 |
| 虚拟化 | 支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合,提供官网截图 |
| 多业务扩展能力 | 支持与路由器一体化的防火墙、IPS等安全业务插卡，需需提供官方网站截图，并提供板卡信息 |
| IPv6 | 具备IPv6能力，所投机框需提供IPv6ReadyII证书 |
| QOS | 支持优先级Mark/Remark、CAR（CommittedAccessRate）、GTS等功能 |
| 为简化ACL配置，设备需支持全局ACL功能 |
| 支持FIFO、PQ、WFQ、LLQ等各种队列调度机制，支持拥塞避免算法：Tail-Drop、RED、WRED，支持层次化Qos（H-Qos） |
| 可靠性 | 支持VRRP/VRRPv3、MPLSTEFRR、IPFRR（静态路由/策略路由/RIP/IS-IS/OSPF等） |
| 为减小设备或线路故障对业务的影响、提高网络的可用性，需支持BFDforBGP/IS-IS/OSPF/LDP/VRRP/StaticRoute，提供第三方测试报告 |
| 支持热补丁功能，可在线进行补丁升级 |
| 为提高设备软件稳定性及可靠性，主备倒换时业务不中断，需要支持NSR功能 |
| 为提高设备硬件稳定性及可靠性，交换网板、板卡、子卡支持热插拔功能 |
| 为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持NQA检测网络网络质量 |
| 网络安全 | 设备支持防攻击能力，包括：ARP攻击、IPv6报文攻击、超大Trace报文攻击、TCPSYNflood、Pingflood、DHCPDDOS、PADIDDOS的防御等 |
| 支持OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的MD5认证功能，支持Keychain功能，可以支持基于时间段的生效的秘钥 |
| 维护特性 | 为方便设备运维管理，设备需内置TCL语言功能，能够解析执行TCL语言脚本 |
| 为方便设备运维管理，设备需内置Python语言功能，能够解析执行Python语言脚本 |
| 为实现设备精细化管理，实现不同进程动态部署到不同的CPU上，设备需支持进程分布式优化功能 |
| 为实现基于角色的权限灵活授权，并且和AAA联动，设备需支持RBAC功能 |
| 为方便设备配置文件管理，设备需支持配置回滚功能 |

* + 1. 出口上网行为管理设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 性能配置 | 产品为标准2U机架式设备，标配不少于4个千兆电口、4个千兆光口SFP+、8个万兆光口SFP+，2个USB2.0接口，1个RJ45串口，性能配置需满足：网络吞吐量≥25Gb，每秒新建连接数≥200000，最大并发连接数≥8000000。 |
| 部署方式 | 支持部署在IPv6环境中，支持所有核心功能（上网认证、应用控制、流量控制等）都支持IPv6。 |
| 实时监控 | 支持针对内网用户的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，提供配置界面截图证明。 |
| 支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略。 |
| 用户认证 | 为满足访客PC的简易接入授权，支持二维码认证，单位担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、免填写信息三种模式。 |
| 网页管理 | 识别并过滤SSL加密的钓鱼网站、非法网站等。 |
| 流量控制 | 支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。 |
| 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。 |
| 应用细分管控 | 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。 |
| 安全审计 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。 |
| 支持网页内容审计后的网页快照功能。 |
| 策略管理 | 支持自动同步现有的上网行为管理设备配置策略，实现与现有设备的无缝对接，降低运维工作量，避免配置遗漏影响现有业务。 |
| 上网安全 | 支持将上网行为管理设备的上网行为及身份信息同步给现有的态势感知平台进行统一分析，便于快速定位中毒主机及人员身份，提供截图证明。 |
| 支持联动现有的态势感知平台进行风险控制，通过现有的态势感知平台即可在风险主机访问浏览器时弹窗提醒对应的用户，或对风险主机的账号进行冻结。 |
| 上网日志管理 | 设备必须支持内置数据中心和独立数据中心。 |
| 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）；支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱。 |
| 支持泄密行为追溯，可以上传文件和关键词，查询有过相关外发记录的人员。 |

* + 1. 市民中心核心网镜像流量设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ✰性能 | ≥1.92Tbps，≥1260Mpps |
| ✰硬件要求 | 配置≥48个10G/1GBASE-XSFP+端口（满配万兆10KM单模模块）,≥2个40GQSFP+端口，≥4个100GQSFP28接口,≥1根3m40GQSFP+电缆 |
| 实配双电源，四风扇 |
| 流量处理 | 支持复制、转发和丢弃，统计计数 |
| 分片报文 | 支持分片报文处理 |
| MAC | ≥256K |
| ARP | ≥92K |
| 兼容性 | 为保证产品兼容性，须与路由器为同一品牌设备 |
| ✰自主可控 | 投标产品为自主可控设备，提供国产化芯片的相关证明材料 |

* + 1. 政务云出口交换机设备

| 指标项 | 指标要求 |
| --- | --- |
| ✰基本性能 | 交换容量≥2.56Tbps，包转发率≥720Mpps |
| 扩展插槽数 | 扩展插槽≥2 |
| 电源 | 模块化双电源 |
| 风扇 | 模块化双风扇，前/后通风，风道可调，提供官网截图或配置手册证明 |
| 设备高度 | 设备机箱高度≤1U |
| ✰性能指标 | 整机路由表项数量≥64k，提供第三方权威机构提供的检测报告 |
| ARP表项数量≥64K，提供第三方权威机构提供的检测报告 |
| MAC地址表项数量≥128K，提供第三方权威机构提供的检测报告 |
| 端口缓存：10M |
| ✰接口类型 | 配置≥24个10G/1GBASE-XSFP+端口（满配万兆10KM单模模块）,≥2个40GQSFP+端口，≥1根3m40GQSFP+电缆 |
| VxLAN | 支持VxLAN二层网关，提供官网截图  支持VxLAN三层网关，提供官网截图  支持EVPN |
| ERPS | 要求支持ERPS功能，并且收敛时间小于50ms，要求提供 |
| 堆叠 | 最大堆叠台数>=9台 |
| 最大堆叠带宽>=480G |
| 支持远程堆叠 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLANID)>=4094 |
| 链路聚合 | 支持最多8个端口聚合；支持最多128个聚合组（IRF2）；支持LACP |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 组播协议 | 支持IGMPv1/v2/v3，MLDv1/v2 |
| 支持IGMPSnoopingv1/v2/v3，MLDSnoopingv1/v2 |
| 支持PIMSnooping |
| 路由协议 | 支持IPv4静态路由、RIPV1/V2、OSPF、BGP、ISIS |
| 支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议) |
| 支持RRPP（快速环网保护协议），环网故障恢复时间不超过200ms |
| 访问控制策略 | 支持基于第二层、第三层和第四层的ACL； |
| 支持基于端口和VLAN的ACL |
| 支持IPv6ACL |
| SDN/OPENFLOW | 支持OPENFLOW1.3标准支持普通模式和Openflow模式切换，需提供官网网站命令手册佐证支持多控制器（EQUAL模式、主备模式） |
| 管理和维护 | 支持SNMPV1/V2/V3、RMON、SSHV2 |
| 支持OAM(802.1AG，802.3AH)以太网运行、维护和管理标准 |

* + 1. 政务网核心路由器（P设备）冷备设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ✰设备性能 | 交换容量≥115Tbps，转发性能≥14000Mpps  要求与原有政务网PE设备华为NE20E完全兼容，可以在NE20E故障后直接替换使用 |
| ✰配置要求 | 本次所投路由器配置要求如下：  1.双主控，双交换网板，双电源  2.万兆光口≥20个，千兆光口≥20个，千兆电口≥8个 |
| ✰设备架构 | 要求所有业务板卡及电源、风扇均可热插拔；整机业务载板插槽≥6个（且单槽位最大支持200G线速转发不丢包） |
| 设备支持100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS等接口类型 |
| 支持端口散列技术，可将100GE端口散列成10GE口或者25GE口进行使用，可灵活进行设备的端口容量和类型控制使用，提供产品手册等材料证明 |
| 基本功能 | 支持RIP、OSPF、IS-IS、BGP等路由协议 |
| 支持L2VPN、L3VPN、EVPN等VPN技术 |
| 支持LDPLSP、RSVP-TE、SR-TE等MPLS技术 |
| 支持VXLAN、GRE等隧道技术 |
| 支持智能隧道CBTS功能 |
| IPv4、Ipv6路由及转发表容量要求：  1、支持IPv4路由表容量≥10M,IPv6路由表容量≥5M  2、支持IPv4转发表容量≥4M,IPv6转发表容量≥2M |
| IPV6演进 | 支持ISISforSRv6 |
| 支持SRv6TEpolicy,支持通过BGP协议创建Policy，支持基于color，DSCP方式引流入SRv6Policy |
| 可靠性 | 支持基于硬件的BFD故障探测技术，支持最小发包间隔5ms |
| 支持LDP,VRRP,OSPF,ISIS,BGP,VRRP6,OSPFv3,ISIS6,BGP4+,MPLSL3VPN,MPLSTE,PIMSM的NSR（不中断路由技术），主备倒换不丢包 |
| 支持VRRP、Eth-Trunk、E-Trunk等可靠性技术 |
| 支持Telemetry，可实现从设备高速采集数据的技术，设备通过推模式（PushMode）周期性的向采集器上送设备的接口流量统计、CPU或内存数据等信息，提升用户进行网络大数据分析能力，需提供官方产品手册中对该功能的描述说明 |
| 支持随流的性能检测技术，即不额外发送检测报文，对用户业务流进行直接的丢包、时延的监测，得到业务端到端或逐跳的丢包和时延信息，支持通过telemetry上送获得的性能数据，需提供官方产品手册中对该功能的描述说明 |
| 支持对随流检测获取到的性能数据进行可视化的管理；支持设置告警阈值，对指标越限的链路、网元和端口进行告警，需提供官方产品手册中对该功能的描述说明 |
| 系统安全 | 支持BGPFlowSpecification及BGPv6FlowSpecification技术 |
| 支持MACSec加密技术 |
| 支持BGP监控协议BGPMonitoringProtocol（BMP）（RFC7854），能够对网络中设备的BGP运行状态进行实时监控，实现针对网络的路由安全追踪，路由事件回溯和网络安全剖析 |

* + 1. 城域网汇聚交换机（涉及4个汇聚机房、热备）设备

| 指标项 | 指标要求 |
| --- | --- |
| 交换容量 | 2.56Tbps |
| 转发性能 | 720Mpps |
| 扩展插槽数 | 扩展插槽≥2 |
| 电源 | 模块化双电源 |
| 风扇 | 模块化双风扇，前/后通风，风道可调 |
| 性能指标 | MAC地址表>=128K |
| 路由表容量>=64K |
| ARP：64K |
| 端口缓存：10M |
| 接口类型 | 支持24个10G/1GBASE-XSFP+端口,支持2个40GQSFP+端口,单台配置不少于12个10KM万兆光模块 |
| VxLAN | 支持VxLAN二层网关  支持VxLAN三层网关  支持EVPN |
| 堆叠 | 最大堆叠台数>=9台 |
| 最大堆叠带宽>=320G |
| 支持跨设备链路聚合，单一IP管理，分布式弹性路由 |
| 支持通过标准以太端口进行堆叠（万兆或40G均支持） |
| 支持远程堆叠 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 最大VLAN数(不是VLANID)>=4094 |
| 链路聚合 | 支持最多32个端口聚合；支持最多128个聚合组（IRF2）；支持LACP |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 组播协议 | 支持IGMPv1/v2/v3，MLDv1/v2 |
| 支持IGMPSnoopingv1/v2/v3，MLDSnoopingv1/v2 |
| 支持PIMSnooping |
| 支持MLDProxy |
| 支持组播VLAN |
| 支持PIM-DM，PIM-SM，PIM-SSM |
| 支持MSDP，MSDPforIPv6 |
| 支持MBGP，MBGPforIpv6 |
| 路由协议 | 支持IPv4静态路由、RIPV1/V2、OSPF、BGP、ISIS |
| 支持IPv6静态路由、RIPng、OSPFv3、BGP4+ |
| 支持IPv4和IPv6环境下的策略路由 |
| 支持IPv6手动隧道、6to4隧道和ISATAP隧道 |
| 支持OAM(802.1AG，802.3AH)以太网运行、维护和管理标准 |
| 绿色节能 | 符合IEEE802.3az（EEE）节能标准 |
| 端口定时down功能（Schedulejob） |
| 支持端口休眠，关闭没有应用的端口，节省能源 |
| 支持智能风扇调速 |
| 提供ROHS节能认证 |
| 资质认证 | 要求提供信产部入网证和检验报告 |

* + 1. 城域网PE交换机板卡

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 配置要求 | 要求本次所投交换机板卡与现有华为7706交换机完美兼容  1.24端口万兆以太网光接口和24端口千兆以太网光接口板  2.光模块-eSFP-GE-单模模块(1310nm,10km,LC)\*24块，光模块-SFP+-10G-单模模块(1310nm,10km,LC)\*24块 |

* + 1. 市民中心AC设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ✰基本性能 | 现有AC扩容，要求与原有AC完全兼容，所投设备支持常规AP最大数量≥6144 |
| 转发性能 | 数据转发性能≥100Gbps |
| ✰端口要求 | 千兆电端口≥8个  SFP+/SFP端口≥12个  QSFP+端口≥4个 |
| 提供USB接口，配合U盘使用，可用于开局、传输配置文件、升级文件等 |
| 电源 | 应支持双电源备份，并支持交流供和直流二种供电方式。支持电源模块热插拔 |
| 认证加密 | 支持防PSK暴力破解，当用户密码错误超过预设的阀值之后，能够将该用户加入动态黑名单，一段时间内禁止其接入网络，要求提供权威机构的第三方测试报告 |

* + 1. 市民中心吸顶AP设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ✰工作模式 | 采用整机双频4流设计，可同时工作在802.11a/b/g/n/ac/acwave2/ax模式。 |
| ✰协商速率 | 整机协商速率≥1.775Gbps，其中5G射频速率≥1.2G，2.4G速率≥0.575G。 |
| 接口设计 | ≥1个10/100/1000Mbps(RJ45)。 |
| 接入规格 | 整机接入用户规格1024，要求提供官网链接以及官网截图证明。 |

* + 1. 市民中心面板AP设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ✰工作模式 | 采用整机双频4流设计，可同时工作在802.11a/b/g/n/ac/acwave2/ax模式 |
| ✰协商速率 | 整机协商速率≥1.775Gbps，其中5G射频速率≥1.2G，2.4G速率≥0.575 |
| 接口设计 | 整机接口≤1个10/100/1000Mbps(RJ45)千兆接口，设备不提供有线下行口。 |

* + 1. 电子政务外网专业DNS服务设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件规格 | 采用2U机架式专用硬件平台；采用2U冗余电源配置；固定业务接口，不低于6个千兆电口；2个万兆光口，存储介质，企业级存储介质、容量1TB |
| 性能要求 | DNSQPS指标不低于10万/秒 |
| 高可用性 | 部署方式：旁路模式部署，设备在客户实际网络中进行设备测试和验证过，以确保设备具备实际网络适用性 |
| 设备必须支持高可靠，高可用，支持HA自动切换功能和active-standby模式 |
| 渗透防护 | 支持登录认证页面产生加密随机数，可以和Session会话进行对比分析，预防CSRF攻击 |
| 一键断网 | 特殊时期或者网站出现问题的时候，通过该功能随时随地实现“一键断网”管理，中止服务器对外提供服务。支并持自定义设置资源关闭或开启的时间（提供产品运行时操作界面截图） |
| NTP服务 | 支持NTP协议，RFC1119、RFC1305等 |
| 支持通过NTP协议进行IP/MAC活跃度审计，审计信息包括：源客户端IP/端口，源客户端MAC地址，目的IP/端口，ETH网卡 |
| 管理功能 | 用户界面支持中文 |
| 支持双因子登录鉴别，支持动态令牌种子文件的导入，支持动态令牌+用户名/密码方式，防止密码重放性攻击 |
| 支持操作日志的完整记录与查询，包括登录日志和DNS配置变更日志等 |
| 支持将DNS等外部数据方便的导入，支持.xls和.xlsx格式 |
| 支持SYSLOG日志发送第三方日志服务器，可以配置日志发送的级别 |
| DNS功能 | 支持对NS、SOA、A、AAAA、MX、CNAME、DNAME、TXT、PTR、SRV、NAPTR等记录的解析 |
| 标准DNS服务：系统必须支持标准的DNS服务 |
| 反向DNS解析：支持反向DNS解析功能 |
| 支持DNS主从实时备份机制，支持DNS全局和区域转发 |
| 支持DNS参数定义（如allow-transfer、allow-recursion、allow-query、allow-notify、acl、MinimalResponses、check-names、RRSet-Order、ServerTSIGkey等参数） |
| 中文域名支持：支持中文域名，为企业定制中文的内部域名体系 |
| 支持IPv6，DNS解析服务支持IPv6 |
| 多级部署：支持域名服务系统的分布式部署，各节点数据统一下发，并能保证数据一致性 |
| DNS负载均衡：支持DNS负载均衡，支持DNS记录轮循 |
| DNS缓存处理：支持对缓存记录的显示管理，且能针对缓存记录进行删除 |
| 支持泛域名解析：支持泛域名解析，可有效防止用户输入错误而导致网页无法打开的问题 |
| URL重定向：支持URL重定向功能，便于将繁琐较长的网站转成较短的网址 |
| DNS解析排序：支持解析结果按照管理员设定的ISP所属网段返回，实现解析结果链路类型的负载应答控制 |
| DNS智能解析：支持设定网通、电信、移动、教育、科技网等IP地址段，针对不同的地址段解析不同的IP，便于外部访问主页提高访问速度 |
| DNS安全加固优化，支持配置操作系统资源限制，支持配置TCP最大连接数量，支持配置递归查询最大数量，支持配置缓存Cache可用数值，支持启用/关闭DNSSEC/EDNS |
| 具有丰富的DNS解析日志及统计报告，所有节点DNS解析实时展示和统计，实时展现服务设备访问的并发数据，通过饼图、柱状图进行清晰展现，帮助网络管理员跟踪和快速解决与DNS配置有关的问题。包括QPS、Top域名、TopIP、解析记录统计；支持基于中国和世界的DNS访问排名统计分析 |
| DNS安全 | 支持禁止DNSANY类型请求，支持防止DDOS攻击和放大攻击，支持基于IP或域名进行请求限速，支持自定义规则；  支持DNS高性能防护，支持配置QPS告警阈值，当业务量突增能够自动关闭查询日志来保证DNS核心功能解析；  支持DNS响应策略，支持恶意域名的识别和过滤，针对域名进行阻断，支持域名不存在/存在无响应/不启用策略/强制TCP/丢弃/域名劫持等操作；  支持启用DNS隧道攻击防护，支持限制隧道攻击源IP地址范围，提高攻击者的信道部署代价；  针对域名劫持，支持对重点域名的资源记录进行监测，同时定义重点域名对应的IP地址群，当有变化的时候，且变化后的内容不在给定的IP地址群中，则输出日志，发送告警信息； |
| 支持DNS黑名单，自定义待过滤黑名单IP，实时生效 |
| 支持DNS域名过滤，自定义域名URL，实时生效 |
| 支持显示和下载已定义恶意域名的访问命中率报表 |
| 支持定义TSIG，确保Zone转换、Notify、动态升级更新、递归查询邮件等DNS消息的安全，预防DNS欺骗 |
| 支持DNSSEC，支持ZSK和KSK更新策略，支持定义密钥启用时间，不启用时间和终止时间 |
| 支持DNSQPS性能超过阈值告警功能，支持DNSQPS查询阈值设定 |

* + 1. 电子政务外网专业DHCP服务设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件规格 | 采用2U机架式专用硬件平台；采用2U冗余电源配置；固定业务接口，不低于6个千兆电口；2个万兆光口，存储介质，企业级存储介质、容量1TB |
| 性能要求 | DHCPLPS指标不低于2000/秒 |
| 渗透防护 | 支持登录认证页面产生加密随机数，可以和Session会话进行对比分析，预防CSRF攻击 |
| 一键断网 | 特殊时期或者网站出现问题的时候，通过该功能随时随地实现“一键断网”管理，中止服务器对外提供服务。支并持自定义设置资源关闭或开启的时间（提供产品运行时操作界面截图） |
| 高可用性 | 设备必须支持HA（high-availability）自动切换功能和active-standby模式 |
| 管理功能 | 用户界面支持中文 |
| 支持双因子登录鉴别，支持动态令牌+用户名/密码方式，防止密码重放性攻击 |
| 支持将外部数据方便的导入，支持.xls和.xlsx格式 |
| 支持将数据库内容实时备份和定时备份 |
| 支持将设备的日志文件的导出 |
| 设备支持和主流的上网行为厂商（深信服、网康）进行接口联动，实现IP/MAC全程审计 |
| 支持实时显示设备CPU负载、空闲内存、磁盘使用、DNSQPS，DHCPv4LPS，DHCPv6LPS等设备参数 |
| NTP服务 | 支持NTP协议，RFC1119、RFC1305等 |
| 支持通过NTP协议进行IP/MAC活跃度审计，审计信息包括：源客户端IP/端口，源客户端MAC地址，目的IP/端口，ETH网卡 |
| DHCP功能 | CIDR（无类域间路由）支持 |
| 支持业界标准的DHCPFailover |
| 支持DHCPOption60/Option82，支持高级DHCP选项编辑器，支持厂商自定义Option |
| 基于IP/MAC地址的静态绑定（IP保留地址分配） |
| 实现地址的动态分配和回收，实时显示分配地址的状态和续租信息 |
| 支持DHCP系统指纹技术，支持BYOD（BringYourOwnDevice），自动识别智能手机、平板电脑等的系统指纹 |
| 支持DHCP指纹识别率98%以上，支持快速对DHCP未知指纹进行识别及添加 |
| 支持所有ISC预定义的DHCPoption空间（如Option1到Option125）和客户化的DHCPOption空间（如Option126到Option254） |
| 支持DHCP参数强制下发，针对于非标准DHCP协议的客户端请求IP地址时确保参数此参数可以下发 |
| 支持DHCP模板功能，快速创建和复制DHCP参数配置 |
| 支持IP地址强制释放功能，针对部分终端DHCP租期到了不会主动续约并继续使用过期IP的情况，实现手工和周期性强制释放IP地址，以确保IP地址的利用率 |
| 支持DHCP实时在线用户趋势分析、DHCP响应包趋势分析、IP数据利用率实时统计分析、DHCP指纹数据实时统计等 |
| DHCP6支持 | 提供IPv6子网掩码计算功能，可计算IPv6网络的起始/终止地址、划分后的子网数量、划分后的前5个子网（提供产品运行时操作界面截图） |
| 支持DHCPv6保留地址分配，支持DUID绑定，支持批量绑定 |
| 支持DHCPv6客户端参数设定，支持无状态地址信息刷新时间设定 |
| 支持DHCPv6有状态地址分配，支持自动发现设备DUID标识 |
| IP地址管理 | 支持对IP数据进行统一集中管理，支持IPv4和IPv6双协议栈，支持分级分权管控，不同用户可管理不同范围的IP地址 |
| 支持IP地址规划，可以自定义分区域进行IP地址规划，包括子网划分等功能 |
| 支持地址扫描，提供子网中IP地址的可用性状态，可以定期对IP地址的在线状态进行检查，避免地址冲突。IP地址分配情况自动统计 |
| 要求支持图形化IP地址分配；支持基于IP地址的网络视图，能够轻松查找子网；从子网中标记IP地址的使用情况，保留、已分配等 |
| 支持按照不同字段搜索功能，支持模糊搜索，IP地址系统可以支持IP地址、MAC地址、设备名称的查询 |
| 支持IP地址回收功能，对于检测到的长期不使用的IP地址，系统可以自动或者手动回收 |
| 支持查看IP地址分配的历史明细及相关记录，具有IP地址分配审计功能，能够记录执行操作的用户、所做变更、时间等。 |
| 系统支持定义地址调和核查策略，形成基线对比，可以配置时间策略对比物理网络和IP地址管理系统内的地址变更情况 |
| 支持发现未知IP核查状态，此状态表明此IP由于各种原因没有被记录在系统中，如非法接入、手动私设地址等 |
| 支持待清除核查状态，此状态表明此IP地址长时间没有被使用 |

* + 1. 短信服务

每年短信服务支持不少于20W条。

* + 1. 公共接入区防火墙设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 性能参数 | 2U机箱，冗余电源，标准配置板载16个10/100/1000M自适应电、6个SFP光接口和8个SFP+光接口（支持兼容千兆光口）,1个Console口，一个HA口；另外含有4个扩展插槽，支持液晶屏。网络处理能力60Gbps，并发连接≥1200万，每秒新建连接45万/秒。包含应用控制、病毒防护、入侵防御特征库服务。  含8口千兆板卡两块 |
| 系统架构 | 硬件设计采用高性能一体化智能安全处理引擎 |
| 部署模式 | 支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式 |
| 网络协议 | 支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议 |
| 路由协议 | 所投产品必须支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，支持基于优先级的ISP路由链路备份；支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试（需要提供能够体现上述功能及配置选项的截图） |
| 高可靠性 | 所投产品必须支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；支持链路探测 |
| 应用识别与控制 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类（需要提供能够体现上述功能及配置选项的截图）为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类 |
| 用户识别与认证 | 所投产品必须支持基于用户的访问控制，可与LDAP/Radius/证书/Active Directory/TACACS+/POP3等用户认证系统联动 |
| 所投产品必须支持802.1x认证，要求支持基于端口和MAC两种接入控制方式；所投产品支持管理用户、VPN用户、WebAuth用户的双因素认证；  支持二层MAC地址IP地址绑定；支持跨三层MAC地址IP地址绑定 |
| 文件过滤 | 所投产品必须支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件五种分类；（需提供支持的应用分类和对应的设备配置截图） |
| 所投产品必须支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等30种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别 |
| 流量管理 | 所投产品必须支持多调度类相互嵌套最大5级的带宽管理设置。支持设置每IP最大或最小带宽，支持对每IP进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配 |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀（需提供支持的应用分类和对应的设备配置截图）；  本地病毒库规模大于3000万；支持对最多6级的压缩文件进行解压查杀  支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| 共享上网检测 | 所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作 |
| 运维管理 | 所投产品必须支持业务接口下Netflow功能，能够通过Netflow实现对网络进行监控，对接口流量进行抓包，并在可将Netflow抓包文件数据外发（投标文件需提供能够体现上述功能及配置选项截图） |
| 所投产品必须支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理，支持通过设置IP地址、MAC地址、资产类型、操作系统、应用、开放的端口和访问的端口等信息来制定资产指纹库 |

* + 1. 公共接入区数据安全交换系统设备

1. 包括数据交换前置机、隔离网闸和数据交换后置机三部分组成。系统设计采用一种基于FPGA和DSP的国密加密安全数据交换卡及交换方法；产品厂商入围《通过公安部组织测试的接入平台厂商名单》；产品通过公安部信息安全等级保护评估中心检测；
2. 数据交换前置机与数据交换后置机网络接口分别为：千兆电口≥6，万兆光口≥2；隔离网闸网络接口：千兆电口≥12，万兆光口≥4；
3. 交换能力：≥8Gbps；并发会话：30000个；数据库到数据库交换记录数（>100Kb/记录）：≥10300条/秒；数据文件处理文件数（>100Kb/记录）：≥1500个/秒；数据文件处理吞吐量：≥8Gbps；应用层数据交换速度（FTP）：≥800Mbps；最大数据文件：≥30G；任务调度粒度：秒级；目录监控触发时间：<1秒；最大传输延时：<30ms；
4. 支持主流数据库交换，包括：Oracle、DB2、SQL Server、Sybase及MYSQL的各种版本，支持国产数据库如：达梦、神舟通用等；
5. 支持多种数据库获取方式，包括：全表镜像模式、增量模式、快照日志模式、触发器模式和同表双向模式；
6. 支持各种数据库之间的异构数据转换，包括：不同数据库、同类数据库不同版本的转换、异构表、异构字段名、异构字段类型的转换、异构字符类型、异构数据库字符集的转换、大字段的异构等；
   * 1. 公共接入区视频安全交换系统设备
7. 由视频用户认证服务器、安全隔离设备和视频接入认证服务器三部分组成。用于支撑可信网络内的用户安全访问不可信网络中的视频资源。产品通过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 产品获得公安部销售许可证，产品获得公安部安全与警用电子产品质量检测中心检测，产品厂商入围《通过安全测评的视频安全交换产品及厂商目录内厂商生产产品》；
8. 视频用户认证服务器：性能要求：千兆电口≥6，万兆光口≥2；支持2000路D1图象（2Mbps）或≥1000路高清（4Mbps）；网络吞吐量≥4Gbps；
9. 功能描述：提供基于https的图形化安全管理，支持用户名/口令、数字证书等多种认证管理方式；管理员及审计员区分并独立，支持分权管理，对管理员角色定制，可以添加多个管理员角色，并定制权限；支持管理员登录失败锁定次数、锁定时间和超时时间的设定；通过界面能够查看到多核CPU使用率、设备运行状态检测、系统资源监控；视频分辨率支持D1、VGA、2/3D1、1/2D1、SIF等多种分辨率，具有低延迟、低丢包率等特性；支持视频压缩标准：MPEG4、H.264等数字图像编解码标准；
10. 视频接入认证服务器：性能要求：千兆电口≥6，万兆光口≥2；支持2000路D1图象（2Mbps）或≥1000路高清（4Mbps）；网络吞吐量≥4Gbps；
11. 安全隔离设备：性能要求：千兆电口≥12，万兆光口≥4；网络吞吐量≥4Gbps；
12. 视频专网隔离区专用网闸，系统内部采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块；内外端机为网络协议终点，彻底阻断各种网络协议，保证信任网络和非信任网络之间链路层的断开，彻底阻断TCP/IP协议以及其他网络协议；
    * 1. 机房优化

将机房中政务云节点搬迁至运营商机房，并且对机房进行优化，满足实际要求。

* + 1. 一键封堵

1. 实现和安全管控平台对接，对政务外网实现一键封堵。
2. 实现市政务外网基础网络边界设备的一键封堵，做到7\*24小时不间断封堵，支持对接第三方平台。
   * 1. 省市边界防火墙

|  |  |
| --- | --- |
| 指标项 | 功能参数 |
| 性能参数 | 下一代防火墙系统软件；含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN；多核AMP+架构，网络层吞吐量≥60G，并发连接≥850万，每秒新建连接数≥60万，标准2U机箱，冗余电源， 标准配置1个Console口 、1个HA接口，1个MGT接口，4个万兆光口，支持2路万兆光口bypass；支持3个扩展插槽；支持液晶屏。含硬件维保服务，全功能模块升级订阅服务包（含应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务） |
| 部署模式 | 支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式 |
| 网络协议 | 所投必须支持MPLS流量透传，对带有MPLS数据包流量进行封装/解封装，对数据包内容进行安全检查和分析，进而按照既定安全策略，进行转发和抛弃处理，对于转发的数据包还原标记并进行封装转发。支持针对MPLS流量的安全审查，包括漏洞防护、防病毒、流量控制、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能；（提供功能截图证明） |
| 路由协议 | 所投产品必须支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，支持基于优先级的ISP路由链路备份；支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |
| 高可靠性 | 所投产品必须支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；支持链路探测 |
| 网元管理 | 支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如WAF安全资源池），并将流量通过负载均衡的方法编排给组内所有网元 |
| 服务链配置 | 支持灵活的服务链编排配置，支持串接链和旁路链，支持网元组的方向和位置设置 |
| 引流功能 | 支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志 |
| 编排流量监控 | 支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计 |
| SSL 解密 | 支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4和IPv6地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计（提供功能截图证明） |
| 运维管理 | 所投产品必须支持业务接口下Netflow功能，能够通过Netflow实现对网络进行监控，对接口流量进行抓包，并在可将Netflow抓包文件数据外发 |
| 所投产品必须支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理，支持通过设置IP地址、MAC地址、资产类型、操作系统、应用、开放的端口和访问的端口等信息来制定资产指纹库 |
| 第三方对接 | 支持提供IP地址封禁、解封的相关接口至第三方平台进行IP地址联动封禁 |

* + 1. 运维区防火墙

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 资源配置 | 性能不低于：网络层吞吐量：15G，应用层吞吐量：8G，防病毒吞吐量：1G，IPS吞吐量：1G，全威胁吞吐量：800M，并发连接数：200万，HTTP新建连接数：9万。 |
| 软件要求 | 含WEB应用防护识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和URL&应用识别库； |
| 路由支持 | 产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 |
| 产品支持IPsec VPN和SSL VPN功能。 |
| 产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。 |
| 为满足组网兼容性，IPSec VPN需支持IKEv1和IKEv2协议，支持基于主模式和野蛮模式建立加密隧道。 |
| 为满足业务未来组网要求，投标人所投产品应支持IPSec VPN智能选路功能，根据线路质量实现自动链路切换。（提供界面截图证明） |
| 用户识别与认证 | 产品支持多种用户认证方式，用户认证方式要求支持本地密码认证、外部密码认证和单点登陆等方式。 |
| 应用控制 | 为满足业务人员安全防护要求，投标人所投产品应支持对各种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（提供界面截图证明） |
| 产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。 |
| 产品支持基于IP对象的会话控制策略，实现并发连接数的合理限制。 |
| 访问控制 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 安全防护策略 | 产品支持全面的URL分类库，针对网站类别实现细粒度管控，杜绝非法、违规网站的访问行为。 |
| 产品支持对文件传输行为进行安全过滤，支持基于上传、下载、双向的文件内容过滤，内容过滤类型至少支持网页、脚本、压缩文件、图片、可执行文件、适配、文本等常见文件类型。 |
| 产品内置不低于10000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。 |
| 产品支持对HTTPS协议加密流量进行解密，支持配置基于区域、对象、业务类型、服务器IP/端口的解密策略。 |
| 产品支持勒索病毒检测与防御功能。 |
| 压缩文件病毒防护：产品支持对多重压缩文件的病毒检测能力，支持不小于15层压缩文件病毒检测与处置。 |
| 僵尸网络防护：产品支持僵尸网络与病毒防护功能功能，产品预定义特征库超过150万种。 |
| 漏洞防护：产品内置不低于10000种漏洞规则，提供漏洞防护能力。 |
| 产品支持CC攻击防护功能。 |
| 产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。 |
| 产品支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制。 |
| 安全策略管理 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 支持联动现有的态势感知平台，同步链路信息日志、上报CPU、内存、网卡流量等信息，实现通过现有平台进行设备的集中管理、集中监控、多日志关联分析。（提供界面截图证明） |
| 高可用性 | 产品支持主主、主备两种双机模式部署。 |
| 第三方对接 | 支持提供IP地址封禁、解封的相关接口至第三方平台进行IP地址联动封禁 |

* + 1. 电子政务外网违规外联检测设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件规格 | 采用高性能规格的机架式1U硬件设备，全内置封闭式结构，专用安全加固Linux操作系统。 |
| 硬件参数 | 处理器：Intel酷睿i7，内存≥16GB（最大支持16GB\*2），硬盘：≥128GB硬盘，网络接口：≥6个千兆电口，≥2个万兆光口，其他接口：≥1个VGA接口，≥2个USB接口。 |
| 性能指标 | 最大镜像流量：20Gbps，最大扫描扫描速率：50Mb/s |
| 内外网互联 | 1.在无需安装客户端的情况下，支持通过镜像流量分析自动发现管理域内同时连接内网和互联网的设备，可在外联服务器上取证，取证信息包含外联设备内网IP、外联出口IP、首次发现时间和最后更新时间等信息。  2.支持在外联服务器上取证，取证信息包含：外联设备内网IP、外联出口IP、发现次数、首次发现时间和最后更新时间等信息。  3.支持数据在外联告警系统与内网管理系统间的导出和导入。 |
| 非授权外联 | 1.在无需安装客户端的情况下，支持自动发现管理域内曾经脱离内网并且连接过互联网的设备，可在外联服务器上取证，取证信息包含外联设备内网IP、首次发现时间和最后更新时间等信息。  2.支持在外联服务器上取证，取证信息包含：外联设备内网IP、外联出口IP、发现次数、首次发现时间和最后更新时间等信息。  3.支持数据在外联告警系统与内网管理系统间的导出和导入。 |
| 线路外联 | 1.支持在不依赖于客户端技术的情况下，自动发现管理域内内网网络设备（如：交换机、路由器等）与其他网络（如：互联网）相连，造成大量内网设备外联的情况。（需提供公安部信息安全产品检测中心等权威测评机构对该项功能的检测结果作为证明）。  2.支持在外联服务器上取证，取证信息包含：外联设备管理口IP、外联设备MAC、外联出口IP、发现次数、首次发现时间和最后更新时间等信息。  3.支持识别外联设备的厂商信息，辅助对外联设备进行定位和取证。  4.支持数据在外联告警系统与内网管理系统间的导出和导入。 |
| 网页外泄 | 1.支持自动发现管理域内将内网应用系统或网站页面保存后，拷贝至其他网络（如：互联网）计算机打开的疑似信息外泄行为。  2.支持在外联服务器上取证，取证信息包含：设备内网IP、外泄时外网IP、首次发现时间、最后更新时间和外泄网址等信息。  3.支持数据在外联告警系统与内网管理系统间的导出和导入。 |
| 外联事件辅助查证 | 支持配置内网IP归属区域信息，与发现的外联信息关联分析，提供外联IP的网络归属，可辅助外联行为的调查。 |
| NAT接入 | 支持自动发现管理域内的NAT设备和通过该设备私自搭建的局域网，同时上报其边界点设备IP地址、运行状态、首次发现时间、最后更新时间等信息，并能发现NAT子网中设备的IP地址等信息。 |
| 移动设备接入 | 在支持不依赖于客户端技术的情况下，支持自动发现管理域内的移动设备接入行为，上报设备的IP、操作系统、厂商类型等信息。 |
| 边界备案 | 支持对上报的边界点进行人工备案管理，包括完善其边界基础信息，明确其责任人、责任部门、联系电话、用途等信息，通过人工报备方式对已知边界进行人工备案管理。 |

* + 1. 电子政务网态势感知设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ✰基础性能 | 不低于以下要求：  性能参数:存储容量:32T，在带宽性能1Gbps时存储时长:1800天/1Gbps。  硬件参数:规格:2U，内存:8\*32GB；系统盘:1\*240GBSATASSD，数据盘:12\*4TB，标配盘位数:12，电源:白金，冗余电源,接口:6千兆电口+2万兆光口。 |
| 部署功能 | 支持与原有态势感知集群化部署，提高态势感知平台整体性能。 |
| 大屏功能 | 支持不同安全视角展示16个独立的大屏展示功能，包括全网安全态势感知大屏、分支安全态势、安全事件态势、通报预警态势、资产态势大屏等，同时能满足多种场景的监控，比如日常运维、护网场景。提供产品界面截图。 |
| 可基于数据中心、总部、租户等按照风险等级（优秀、良、中、差）来展示数据中心的情况。支持对数据中心正常反问的趋势和攻击者监视和分析威胁的说明。 |
| 资产中心 | 支持自定义分支管理权限，分支管理员具备独立的管理页面，只能管理和查看所属分支的业务和终端资产的安全信息且具备完整的功能展示。 |
| 支持资产属性重新识别，当发现资产数据不准确时，可清空该资产属性，如主机名、备注、操作系统、标签、地理位置、硬件信息、应用软件信息、账号信息、责任人信息、端口信息等，重新发起识别后，平台会自动补齐资产属性，可批量操作。 |
| 支持跨三层取MAC地址，识别资产MAC地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题。 |
| 脆弱性管理中心 | 弱密码检测技术基于UEBA学习技术（无监督自我学习）提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征。 |
| 弱密码检测规则支持高度自定义，包括规则名称、生效域名、长度规则、字符规则、字典序、web空密码、账号白名单、密码白名单、txt文件格式导入。 |
| 支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web应用等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。 |
| 威胁分析检测 | 支持DNS服务器日志导入，可以接入DNS服务器的日志，安全分析引擎将结合DNS服务器的日志，定位出DNS服务器代理风险外连场景下真实源IP，从而有效地进行风险处置闭环。 |
| 能够针对HTTP、FTP、LDAP、VMWARE、ORACLE、VNC等弱密码协议进行检测，提供具备CMA（中国计量委员会）认证的第三方权威机构相关检测报告。提供产品报告截图。 |
| 具备恶意文件的检测引擎，对已知家族变种的查杀能力强。如勒索病毒检测达到业界领先的检出率，包括影响广泛的WannaCry、BadRabbit等病毒； |
| 工单系统 | 支持随机生成临时管理员用户名和密码，随机用户名为临时自动创建管理员，只具备指定资产对应的：处置中心、脆弱性、日志检索的查看和操作权限，具备处置、上传附件等下级管理处置的权限。 |
| 支持下级管理员批量认领上级通报的事件，新增“实际处理时间（天）”，从工单认领开始计时，当处理时间超时，显示：实际处理天数/超时天数。 |
| 设备对接 | 支持SIEM日志关联分析结果的可视化展示。支持第三方日志源接入包括syslog、snmp、kafka等常见类型，提供产品界面截图。 |
| 重保中心 | 具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理。实战阶段的实时攻击分析，实时展受害者IP、攻击者IP、XFF、攻击结果、攻击次数、事件类型、威胁等级、联动响应、状态码、确定性等级等20个以上类型。 |
| 支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，能够直观的看到失陷主机的威胁影响面。 |
| 支持综合安全风险、主机安全风险、脆弱性感知、外部感知、工单、摘要、处置报告多种方式呈现，也支持自定义时间导出PPT报告。可快速生成月度、季度、年度PPT报表。 |
| 产品资质 | 具备中国信息安全测评中心颁发的“国家信息安全漏洞库”兼容性证书。 |

* + 1. 市民中心数据流量探针设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 性能配置 | 不低于以下要求：标准2U机架设备，网络吞吐量≥3Gbps，内存≥32G，接口不少于6个千兆电口、2个万兆光口，冗余电源。 |
| 部署模式 | 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响。 |
| 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。 |
| 流量采集 | 支持对全流量进行采集、检测和提取，具备IDS检测功能，并能将提取到的数据上报给现有的安全感知平台，上报的内容需包括http、DNS、SMB协议审计日志，违规访问日志，漏洞利用日志等。 |
| 基础检测功能 | 具备报文检测引擎,具备多种的入侵攻击模式或恶意UR监测模式。 |
| 网站攻击检测 | 支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL等网站攻击检测。 |
| 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。 |
| 高级检测 | 支持多种类型日志传输模式,必须包含标准模式、精简模式、自定义模式，以适应不同应用场景需求。 |
| 支持传输协议审计日志，必须包括https协议日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志等。 |
| 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。 |
| 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。 |

* + 1. 电子政务外网VPN设备

|  |  |  |
| --- | --- | --- |
| 控制中心 | 性能 | 性能参数：最大理论加密流量：600Mbps，最大理论并发用户数（个）：6000，最大理论https并发连接数（个）：60000，理论https新建连接数（个/秒）：400。 硬件参数：规格：1U，内存大小：16G，硬盘容量：128G SSD，电源：冗余电源，接口：6千兆电口+4千兆光口SFP。 |
| 设备部署 | 为了满足灵活部署的要求，控制中心应支持IPV4/IPV6双栈网络IP配置，可自主选择配置LAN口或WAN口。为了保护设备的安全，可支持默认限制所有IP通过WAN口访问系统，支持通过配置IP白名单的方式来放通WAN口接入的特殊需求。 |
| 资源发布能力 | 通过隧道模式，可以支持基于TCP、UDP、ICMP等协议代理访问业务资源，支持发布IP、IP范围、IP段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面。 |
| 通过WEB模式，可以支持基于http或https协议代理访问业务资源，支持发布IP或域名形式的后端服务器地址，可配置业务应用的具体访问URL路径。 |
| 系统应支持针对发布的WEB应用开启WEB水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用，有效预防数据泄露。 |
| 在业务应用兼容性良好的情况下，支持以隧道模式发布http/https协议的资源，以增加在隧道模式下发布的资源的URL级别审计能力，同时支持为隧道资源添加WEB水印以及单点登录功能。 |
| 客户端兼容性 | 为了不改变原有使用习惯，保障使用体验，需支持以下主流浏览器访问WEB资源：  1、支持IE8及以上版本浏览器访问WEB资源  2、支持Chrome 69及以上版本访问WEB资源  3、支持Edge、Firefox、Opera、Safari等其他主流浏览器访问WEB资源  4、支持微信内置浏览器、钉钉内置浏览器访问WEB资源  5、支持Android、iOS各大手机厂商的自带浏览器访问WEB资源  6、支持国产操作系统浏览器接入并访问WEB资源 |
| 为了保障未来在国产化终端上的正常业务访问，客户端应兼容主流国产硬件CPU的国产操作系统终端，包括但不限于麒麟V10×龙芯、麒麟V10×龙芯LoongArch、麒麟V10×飞腾、麒麟V10×鲲鹏、麒麟V10×兆芯、麒麟V10×海光、麒麟V10×海思麒麟；统信V20×龙芯（3A3000、3A4000）、统信V20×龙芯（3A5000）、统信V20×飞腾、统信V20×鲲鹏、统信V20×海光、统信V20×兆芯等。  提供不少于国产化终端接入授权50个。 |
| 终端接入能力 | 支持不同平台的终端同时在线，管理员可分别设置可同时在线的PC或移动终端个数，配置范围不小于0-1000，当超过终端个数时，可以注销最早登录的终端，且被注销的终端有对应的注销提醒；  管理员可设置允许终端在线数为0，以禁止用户通过此类终端接入访问。 |
| 支持终端设备可视管理  1、支持用户自助查看在线或离线终端列表，并注销其他终端，避免账号盗用；  2、支持查看同账号登录过的终端信息，包括但不限于设备名称、设备系统类型、接入地址、最后登录时间等。 |
| 为了提升系统维护的便利性，管理员可配置是否允许用户通过短信验证码等方式自助找回密码。用户在PC端和手机端的登录页面均可通过点击忘记密码来重置密码。 |
| CDN接入能力 | 支持配置CDN作为客户端下载地址，以降低设备本身的非业务访问带宽压力。支持获取CDN加速前的访问IP，并在日志中记录此IP为客户端IP。 |
| 可信应用 | 为有效防止木马入侵系统后攻击服务器，系统内置了一些常见攻击工具进程黑名单，降低被攻击的安全风险。 |
| 1、管理员可根据采集到的进程信息选择信任/不信任  2、支持管理员自定义可信/不可信的进程 |
| 支持对所有采集到的进程信息、管理员的处理进度进行统计。包括但不限于：全部进程，以及常见攻击工具/孤立进程/未签名进程/未知风险的进程数量；管理员未处理的常见攻击工具/孤立进程/未签名进程/未知风险的进程数量 |
| 虚拟专线 | 针对Windows系统用户，支持配置虚拟专线功能，当用户登录客户端之后，自动断开互联网连接，避免互联网威胁影响内网业务系统。 |

* + 1. 内网数据防护设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 性能配置 | 产品不少于4个千兆电口、4个万兆光口SFP+，支持2个USB口和1个RJ45串口，1U机箱。网络层吞吐量≥1.2Gb，最大并发数≥40万。 |
| 部署方式 | 支持旁路模式，无需更改网络配置，实现数据安全审计。 |
| 统一监控 | 支持向态势感知平台上报设备CPU、内存、上下行流量、上报数据量等状态。 |
| IPv6支持 | 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置。 |
| 上网安全 | 对私接无线上网的行为管理，要求设备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，匹配管理员配置的热点信任列表，对信任列表外非法接入的热点和终端能够进行阻止上网，支持冻结用户IP，并通过邮件形式告警通知管理员，支持显示以IP或用户名的维度统计一段时间内的趋势图。 |
| 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。 |
| 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。 |
| 应用细分控制 | 1.能够对新浪微博、腾讯微博、网易微博等进行细分控制，如：登录、浏览、发微博、上传附件等；  2.能够对teamview、QQ远程桌面等远程控制应用做细分控制，如：接受对方远程控制；  3.能够对Github、百度网盘、百度文库等网络应用的上传动作进行细分控制；  功能提供截图证明。 |
| URL访问及关键字控制 | 要求设备内置海量的URL地址库，可根据访问URL的网页关键字进行过滤控制，特别对于SSL加密的网页、论坛、BBS上的发帖行为也需要支持关键字过滤控制。 |
| 移动APP审计 | 支持常见论坛（天涯社区、猫扑社区、百度贴吧、新浪论坛、搜狐社区等）、微博（新浪）、新闻评论类（腾讯新闻、网易新闻、搜狐新闻、新浪新闻）的移动APP内容审计。 |
| 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。 |
| 加密证书自动分发 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题。 |
| 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）。 |
| 数据中心 | 要求设备必须支持将审计数据备份到外置数据中心，实现海量存储；支持通过USBKEY方式对数据中心管理员进行身份验证，确保我单位核心数据不会外泄。 |

* + 1. 数据库审计设备

| 指标项 | 指标要求 |
| --- | --- |
| 性能配置 | 所投产品应为软硬件一体化1U机架设备，吞吐量≥3Gbps，SQL处理性能≥30000条SQL/秒，至少具备6个千兆电口、2个千兆光口SFP。 |
| 审计功能 | 支持主流数据库Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、达梦、人大金仓、南大通用等。 |
| 支持同时审计多种数据库及跨多种数据库平台操作。 |
| 支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌。 |
| 允许查看SQL语句会话日志。 |
| 统计功能 | 支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况。 |
| 支持自定义报备拖拽，通过自定义报表拖拽功能可以随意拖拽用户预期的统计报表，帮助用户提升通过高级选项筛选报表的可读性，更方便达到预期效果。 |
| 支持以风险级别、源IP、业务主机、数据库用户、风险类型为维度的数据库风险排行。 |
| 数据库安全 | 支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断。 |
| 支持向现有的安全感知平台同步数据库风险日志、管理员操作日志、正常审计日志等日志信息，实现数据的统一审计和威胁的关联分析，并在现有的安全感知平台上显示接入状态。 |
| 可以对SQL语句进行安全检测，并识别当前的SQL操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。 |
| 支持基于SQL命令的webshell检测。 |
| 日志中心 | 支持审计日志的增量备份、全部备份，支持备份文件转储，转储方式支持FTP、NFS，支持备份文件下载到本地。 |
| 响应方式 | 支持Syslog告警、SNMPtrap告警、邮件告警，短信告警。 |
| 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。 |
| 系统管理 | 支持审计系统用户（组）管理（添加、修改、删除、停用、启用）。 |
| 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 |
| 可以实时监控系统的CPU使用率，内存使用率和磁盘占用率。快速定位系统的负载压力和系统运行状况。 |

* + 1. 电子政务外网与政务云边界防护设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 性能 | 产品采用多核并行处理架构，6个千兆电口、6个万兆光口SFP+，支持冗余电源，2U机箱。  网络层吞吐量≥55Gbps，并发连接数≥420万，每秒新建连接数≥31万。 |
| 功能要求 | 1、基础网络特性 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。  2、具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。  3、支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。  4、支持IPv4/IPv6双栈工作模式。  5、支持IPv6环境的安全策略设置，实现入侵防御、防病毒、Web应用防护等等安全功能。  6、访问控制：支持基于区域、IP地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。  7、支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。  8、应用控制：产品内置应用特征识别库，支持不少于10000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。  9、安全防护 支持SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。  10、支持ARP欺骗类攻击防护。  11、支持对HTTPS协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器IP/端口设置解密策略。  12、产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。  13、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。  14、高级威胁分析 支持将安全日志、应用控制日志等上报到现有态势感知平台上，实现威胁的深度关联分析，提供截图证明。  15、支持联动现有的态势感知平台，可通过态势感知平台联动对风险主机进行封锁，封锁其出入站方向，封锁时间支持自定义。  16、安全策略管理 支持应用控制策略有效性检测，保障策略持续优化。  17、支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。 |

* + 1. 市民中心局委办与电子政务外网边界防护设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 产品采用多核并行处理架构，不少于6个千兆电口、6个万兆光口SFP+，支持冗余电源，2U机箱。 |
| 性能要求 | 网络层吞吐量≥50Gbps，并发连接数≥410万，每秒新建连接数≥30万。 |
| 基础网络特性 | 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| 具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。 |
| 支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。 |
| 支持IPv4/IPv6双栈工作模式。 |
| 支持IPv6环境的安全策略设置，实现入侵防御、防病毒、Web应用防护等等安全功能。 |
| 访问控制 | 支持基于区域、IP地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。 |
| 支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 |
| 应用控制 | 产品内置应用特征识别库，支持不少于10000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。 |
| 安全防护 | 支持SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持ARP欺骗类攻击防护。 |
| 支持对HTTPS协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器IP/端口设置解密策略。 |
| 产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。 |
| 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。 |
| 高级威胁分析 | 支持将安全日志、应用控制日志等上报到现有态势感知平台上，实现威胁的深度关联分析。 |
| 支持联动现有的态势感知平台，可通过态势感知平台联动对风险主机进行封锁，封锁其出入站方向，封锁时间支持自定义。 |
| 安全策略管理 | 支持应用控制策略有效性检测，保障策略持续优化。 |
| 支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。 |
| 产品资质 | 产品具备国家信息安全漏洞库兼容性资质证书，需提供有效证书复印件证明。 |
| 产品具备中国人民共和国国家版权局颁发的关于“账号安全保护、主动防御”功能的软件著作权，需提供有效证书复印件证明。 |

* + 1. 市民中心外围局委办边界（鸿鼎、劳技PE侧边界）设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 产品采用多核并行处理架构，不少于6个千兆电口、6个万兆光口SFP+，支持冗余电源，2U机箱。 |
| 性能要求 | 网络层吞吐量≥50Gbps，并发连接数≥410万，每秒新建连接数≥30万。 |
| 基础网络特性 | 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| 具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。 |
| 支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。 |
| 支持IPv4/IPv6双栈工作模式。 |
| 支持IPv6环境的安全策略设置，实现入侵防御、防病毒、Web应用防护等等安全功能。 |
| 访问控制 | 支持基于区域、IP地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。 |
| 支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 |
| 应用控制 | 产品内置应用特征识别库，支持不少于10000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。 |
| 安全防护 | 支持SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 提供具备CMA认证的第三方权威机构关于“勒索软件通信防护”功能项的检测报告，提供产品报告截图。 |
| 支持ARP欺骗类攻击防护。 |
| 支持对HTTPS协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器IP/端口设置解密策略。 |
| 产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。 |
| 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。 |
| 高级威胁分析 | 支持将安全日志、应用控制日志等上报到现有态势感知平台上，实现威胁的深度关联分析。 |
| 支持联动现有的态势感知平台，可通过态势感知平台联动对风险主机进行封锁，封锁其出入站方向，封锁时间支持自定义。 |
| 安全策略管理 | 支持应用控制策略有效性检测，保障策略持续优化。 |
| 支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。 |

* + 1. 市民中心外围局委办边界（干休所、高银巷PE侧边界）设备

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 产品采用多核并行处理架构，不少于6个千兆电口、6个万兆光口SFP+，支持冗余电源，2U机箱。 |
| 性能要求 | 网络层吞吐量≥55Gbps，并发连接数≥420万，每秒新建连接数≥31万。 |
| 基础网络特性 | 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| 具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。 |
| 支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。 |
| 支持IPv4/IPv6双栈工作模式。 |
| 支持IPv6环境的安全策略设置，实现入侵防御、防病毒、Web应用防护等等安全功能。 |
| 访问控制 | 支持基于区域、IP地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。 |
| 支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 |
| 应用控制 | 产品内置应用特征识别库，支持不少于10000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。 |
| 安全防护 | 支持SYNFlood、ICMPFlood、UDPFlood、DNSFlood、ARPFlood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持ARP欺骗类攻击防护。 |
| 支持对HTTPS协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器IP/端口设置解密策略。 |
| 产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。 |
| 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。 |
| 高级威胁分析 | 支持将安全日志、应用控制日志等上报到现有态势感知平台上，实现威胁的深度关联分析，提供截图证明。 |
| 支持联动现有的态势感知平台，可通过态势感知平台联动对风险主机进行封锁，封锁其出入站方向，封锁时间支持自定义。 |
| 安全策略管理 | 支持应用控制策略有效性检测，保障策略持续优化。 |
| 支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。 |

* + 1. CPE租赁

|  |  |  |
| --- | --- | --- |
| 便携式CPE | 满足主要领导出差访问使用（含国内外1年流量） | 1套 |

* 1. 政务外网平台化运维能力租赁服务

|  |  |  |
| --- | --- | --- |
| 1 | 电子政务外网申请审批服务 | 政务外网VPN申请、墙口开通、有线、无线网络开通关闭，割接报备等流程 |
| 2 | 数据采集服务 | 政务外网设备和政务外网线路相关性能状态数据采集 |
| 3 | 性能自动化告警服务 | 通过web界面中的告警首页，实时展示所有告警状态，告警节点、告警类型和告警内容，使网络管理员能清晰直观的知道网络中存在的问题，快速并准确的对应到告警设备，并对告警内容进行相对应的的处理。 |
| 4 | 数据展示服务 | 可视化呈现拓扑关系，展示对应设备的运行情况、实时展示所选线路信息，线路流量上限、线路实时流量等、按日、周、月统计设备运行情况、按分钟、日统计网络线路流量分布情况、可视化呈现封堵IP数量、黑名单数量、处理告警数量 |
| 5 | 机房管理服务 | 对接机房感知设备，获得机房运行实时情况 |
| 6 | 数据看板对接服务 | 和数字杭州数字数据看板对接，提供所需要的数据 |
| 7 | 政务网线路精细化管理服务 | 对现在的政务外网线路，进行精细化管理，涵盖所有政务网情况，并且提供申请，变更，撤销，提醒等服务 |
| 8 | DHCP数据清洗服务租用 | 存储，查询历史DHCP分配数据，为安全事件溯源提供数据支撑 |
| 9 | 电子政务外网态势感知数据清洗服务租用 | 现有态势感知数据初步清洗后同步至市安全管控平台，为安全管控平台提供可用的网络区域的安全基础数据。 |
| 10 | 骨干网全年无故障率指标服务租用 | 自动采集骨干链路数据形成全年无故障率指标 |

* 1. 市民中心机房设备租赁服务

2.3.1核心及汇聚机房、UPS机房（共8个机房）摄像机、录像机、电子门禁、防盗报警、静电地板吸水贴面、静电消除设备租赁服务。

（1）摄像机

* 汇聚机房摄像机

黑光级1/2.7"CMOS

支持混合补光，人脸抓拍3~6m，普通监控15m

最低照度:彩色：0.0005Lux@（F1.2，AGCON）;黑白：0.0001Lux@（F1.2，AGCON），0LuxwithIR

宽动态:数字宽动态

网络:1个RJ4510M/100M自适应以太网口

防护:IP66

* 核心机房、UPS机房摄像机

黑光级1/2.7"CMOS

支持混合补光，人脸抓拍3~6m，普通监控15m

最低照度:彩色：0.0005Lux@（F1.2，AGCON）;黑白：0.0001Lux@（F1.2，AGCON），0LuxwithIR

宽动态:数字宽动态

网络:1个RJ4510M/100M自适应以太网口

防护:IP66

（2）录像机

* 汇聚机房硬盘录像机

标准机架式

1个HDMI，1个VGA，同源输出，8盘位，2个千兆网口

本次配置2块6T硬盘

* 核心机房、UPS机房监控服务（硬盘录像机）

标准机架式

1个HDMI，1个VGA，同源输出，8盘位，2个千兆网口

本次配置2块6T硬盘

（3）核心及汇聚机房电子门禁服务

* 汇聚机房电子门禁

人脸识别读卡器（银色），3.5寸高清电阻屏，RJ45接口.支持多种开门方式。门禁系统接入机房动环管理平台，能实现记录查看人员出入、开门纪录等操作。

* UPS机房监控（门禁）

1、基于密码技术的非接触式射频IC卡专用门禁读卡器。读卡器硬件CPU部分芯片采用32位ARM技术平台开发的高性能集成芯片，射频部分采用高性能射频芯片，具有读卡速度快、读卡稳定等特点；采用3DES国际标准算法，防止卡片复制，加密性强、安全性高。

2、内置支持SM1算法PSAM模块，保证卡片的绝对加密性。

3、支持通过配置卡灵活配置读卡器的各类输出参数，例如卡片密钥、卡号输出格式、韦根模式、读卡模式等。

4、提供独立密码发卡软件系统，第三方门禁系统不需要作任何修改，即可实现复旦密码与第三方门禁管理系统的无缝对接。

5、密码用户卡的读卡号距离5cm，密码用户卡的读内容距离4cm。

6、读物理卡号在有效距离内数据接收时间小于80ms。密码认证读内容在有效距离内数据接收时间小于200ms。

7、门禁系统含280KG磁力锁，门禁控制器，发卡器等。

（4）核心及汇聚机房防盗报警服务防盗报警

报警主机自带8防区，支持本地8路防区/2线制防区防拆/支持定时撤布防/时控输出。报警主机接入机房现有的管理平台，可以实现远程管理，远程布防。含报警主机、电源、扩展模块、外设、探测器等。

（5）核心及汇聚机房静电地板吸水贴面

静电地板下吸水贴面。

（6）核心及汇聚机房静电消除设备

采用304不锈钢材质，安全稳固，亚导体触摸球体，操作简单，触摸球体3秒以上即可安全有效的消除人体静电，声光报警。

防静电手环防静电性强，安全可靠。

2.3.2 A座3F机房网络柜精密空调租赁服务

1、精密空调额定制冷量12.5kW；EC风机，最大风量3000m3/h;单冷型；支持上下走管；含冷凝水泵；精密空调标配封闭框组件、带式水浸传感器，空调前后全封闭钣金门，带微动开关。

2、精密空调尺寸≤300mm（宽）\*1400mm（深）\*2000mm（高）。

3、精密空调前后门均应为全封闭钣金门，与内部行间空调前送冷风、后回热风的方式相结合，形成冷热通道均密封且互相隔离的效果。

4、精密空调前部内侧应敷设保温棉，减少柜内冷气与室内环境空气发生的热交换，节省空调能耗。

5、精密空调外观与颜色应与机房原有空调外观一致。

6、采用EC变容量压缩机，额定制冷量≥12.5kW（回风温度37℃），应支持在20%～100%冷量范围内按需柔性制冷；

7、列间空调应与利旧空调形成Teamwork群控功能，包括：

主备：一个或几个机组可以被定为备机，当运行的机组发生故障，备用的机组启动运行。

轮巡：机组按照设定的时间轮流运行。

层叠：运行机组不能满足温湿度负荷需要时，启动备用的机组以增加温湿度控制能力。

需求分配：主控设备通过对所有机组的测量数据的监测，计算出群组的总控制需求，按照一定的规则下发给从控设备，作为它们控制的依据或参考。

防止竞争：避免同一机房内多台空调机组同时运行在相反的运行状态（制冷/加热，加湿/除湿），达到节能目的。

8、采用EC风机，最大风量≥3000m3/h，风机数量≥4个，在行间空调正面高度方向均匀分布，水平前部送风背部回风。为保障微模块内气流循环的持续性，风机应采用冗余设计；

9、温度调节范围：18℃~40℃；

10、温度调节精度：±1℃，温度变化率＜5℃/小时；

11、应采用环保制冷剂R410A或R407C；

12、应采用电子膨胀阀，可无级调节开度10%~100%，精确快速地控制流量；

13、制冷剂管路均应支持上下走管；

14、冷凝器工作环境温度范围不小于-15℃～+45℃；

15、冷凝器应能根据冷凝器管道内部压力变化自动调节冷凝风扇的运转速度；

16、冷凝器应具有良好的刚性和防腐性能，适应多种环境条件；

2.3.3 A座3F机房网络柜蓄电池设备租赁服务（部署于负二楼UPS间）

1.单体电池容量：12V100AH；

2.单体电池浮充电压：13.5-13.7V；

3.单体电池均衡充电电压：13.8-14.40V；

4.当蓄电池运行温度在-20--+50℃条件下，其性能指标应满足正常使用要求；

5.蓄电池设计寿命≥10年；

6.阻燃性能：蓄电池间连接条、终端接头应选择导电性能优良的材料，并具有防腐蚀措施。蓄电池槽、盖等材料应具有阻燃性，其阻燃标准应符合YD/T799-2010的阻燃等级要求。

7.蓄电池极性正确，正负极性及端子应有明显标志，便于连接。

8.安全阀动作：蓄电池在使用期间安全阀应自动开启闭合，闭阀压力应在1kPa～10kPa范围内，开阀压力应在10kPa～30kPa范围内；

9.大电流放电：蓄电池在以30I10的电流放电3分钟，极柱不应熔断，其外观不得出现异常；

10.耐过充能力：蓄电池组完全充电后的电池以0.3I10A连续充电160h，无变形、无漏液；

11.荷电保持能力：蓄电池静置28天后，其荷电保持能力不应低于97%；

12.密封反应效率：蓄电池的密封反应效率不应低于98%；

13.防爆性能：充电过程中遇明火、内部不引燃、不引爆；

14.防酸雾性能应满足完全充电后的电池以0.2I10A电流连续再充电4h，PH值应呈中性。

15.封口剂性能应满足环境温度-30℃~+65℃之间，封口剂无裂纹与溢流现象。

16.低温敏感性应满足10h率容量≥0.9C10；外观无破裂、过度膨胀及槽、盖分离现象。

17.电池重量不小于30KG，提供彩页证明。

2.3.4UPS机房消防钢瓶、气体灭火控制盘设备租赁服务

（1）UPS机房消防钢瓶

1、含瓶组、容器阀、压力信号装置、压力表、立柜、转换接头、低泄高密阀、安全阀、高压连接管、喷头、启动装置，每瓶充装药剂110kg。

2、气体灭火柜：充装量120kg；

3、采用柜式结构，静电喷塑；

4、贮存压力：2.5MPa；

5、灭火方式：全淹没；

6、具有手动、自动、机械应急操作启动方式。

7、七氟丙烷纯度99.99%；无色、无味的气体，其臭氧耗损潜能值（ODP）为零，在ISO认可的洁净气体灭火剂中，其洁净性最好，具有清洁、低毒、电绝缘性能好、灭火效率高等特点。

（2）UPS机房气体灭火控制盘

1、气体灭火控制装置，可配接感烟/感温/火焰探测器、手动报警按钮、紧急启/停按钮、声光警报器、气体喷洒指示灯、手自动转换开关以及输出模块等，具有火灾探测和气体灭火控制功能，可实现1个防火区的火灾报警和气体灭火控制。

2、功耗:监视状态功耗≤30W;大功耗≤380W;

3、备用电源:2个DC12V/7Ah密封铅电池;

4、气体喷洒输出:各区DC24V/3A,脉冲方式/持续方式,可调;

5、电池充电电流:1.0A~1.7A;

6、工作电压:交流AC220V50/60Hz,允许电压变化范围C176V~AC264V;

7、液晶屏规格:128×64点,可同屏显示32个汉字信息;

8、使用环境:工作温度:0℃~40℃

9、相对湿度:≤95%,不凝露(10)

10、外形尺寸:宽420mm×厚200mm×高590mm

1. **设备维保服务**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 设备维保服务 | | | | | |  |
| 1 | 市民中心路由交换设备维保服务 | 核心交换机 | H3C S7608X | 2 | 台 | 原厂1年 |
| 核心路由器 | H3C SR-8803-X-S | 2 | 台 |
| 汇聚交换机 | H3CS7506E-NP4 | 4 | 台 |
| 华为S7706 | 4 | 台 |
| 准入认证 | H3C DR2000 | 1 | 套 |
| 2 | 核心PE设备 | 华为NE20E-S8 | 6 | 项 | 原厂1年 |
| P设备 | 华为S7706 | 6 | 项 |
| 汇聚交换机 | 华为 S5730-68C-SI-AC | 12 | 项 |
| 3 | 市民中心机房维保服务 | 机房配电系统 | | 1 | 项 | 原厂1年 |
| 汇聚机房气体灭火系统 | | 3 | 套 |
| 机房精密空调 | | 5 | 套 |
| 机房冷通道动环监控 | | 2 | 套 |
| 部署于市民中心A座3楼机房机房UPS（主机） | | 2 | 台 |
| 汇聚机房(A、B、C、D、E、F)UPS维保 | | 6 | 项 |

▲**投标人必须以承诺函形式在投标文件中承诺在服务周期开始前准时提供完整上述标的物（出口线路，租用的设备和维保），确保杭州市电子政务网络正常运行。否则投标无效。**

1. **其他**

安全责任（中标方义务）

外包服务机构的网络、数据安全责任及违约条款

一、安全责任（中标方义务）

1.中标方应按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规及规章制度的要求，履行网络和数据安全保护义务。

2.本项目所涉及的中标方工作人员均需签订《保密承诺书》，且中标方应对项目涉及工作人员进行背景审查，存在泄密风险的中标方工作人员不得接触项目。中标方应做好人员保密教育工作。

3.中标方应当采取技术措施和其他必要措施，确保其网络和数据安全，防止出现信息泄露、毁损、丢失等风险。在发生或者可能发生信息泄露、毁损、丢失等情况时，应当立即采取补救措施，并将相关情况及时告知采购人。

4.项目中所包含的建设、运营、运维的信息系统、应用、数据库等，中标方开通相关账号、权限等必须经过采购人审批允许，不得私开账号、擅自更改权限等。

5.中标方应合理使用操作账号，严禁中标方存在多名（2人及以上）工作人员共用一个操作账号的情形，同时操作账号应采用高强度的密码，中标方应妥善保管密码并定期更新账号密码。

6.未经采购人允许，中标方不得对项目云资源私开端口，不得利用项目资源进行与该项目无关的工作，不得将政务网和互联网私自打通。

7.中标方应严格按照相关要求收集、归集、存储、加工、传输、共享、开放、利用数据资源。做好数据落地相应的数据保护工作，严格执行数据安全技术标准和安全管理措施，避免相关数据出现篡改、破坏、泄露、丢失、非法利用等风险。

8.中标方应认真组织开展各项数据处理活动，查找项目数据安全隐患和漏洞，对薄弱环节和潜在威胁采取有力措施并进行及时整改，避免和消除数据安全风险，履行数据安全保护义务。

9.中标方应加强网络和数据安全风险监测，制定网络与数据安全应急预案，完善应急机制。一旦发现数据安全缺陷、漏洞等风险时，立即采取补救措施；发生数据安全事件时，立即采取处置措施。确保第一时间监测发现，第一时间应急处置，第一时间向采购人报告。

10.中标方应及时响应、处置采购人布置的安全工作，对其主管的系统、组件、云资源等所属安全事件、隐患及时发现、阻断、排查、处置、溯源（包括但不限于攻防演练等相关活动中发现的）。

11.项目中所建设的系统、提供的基础设施服务等，中标方应无偿提供操作、告警等安全日志以及资产清单，并且按照规范要求与采购人审计平台实现对接，并且提供相关解析服务（如日志字典等）供采购人进行安全审计。

12.中标方派驻的驻场人员应按照采购人要求办理入场、离场等手续，入驻全省ISV系统，并且遵守采购人劳动、工作纪律，按照采购人要求的工作时间进行出勤。

13. 中标方应配合采购人对项目涉及的资源、系统等常态化安全漏洞扫描，并且及时修复漏洞。

14.中标方应配合采购人完成项目中所建设、运营的应用系统、服务等的网络数据安全检查，并且按要求及时完成检查中发现问题的整改。

15.未经采购人允许，中标方不得擅自将项目中涉及的数据拷贝、转移出指定数据区域外进行开发、调试等，包括不限于中标方公司、第三方公司的服务器等。

16．每次通报后，中标方应当及时解决并向采购人提交整改报告并根据整改报告内容进行及时整改。

17.中标方在项目中所承建信息系统的开发、测试环境，不允许出现采购人及项目相关的标识名称，并且在项目建成后及时下架测试环境。

18.中标方应承担在项目运维期中的安全责任，履行运维期的项目、应用系统、云资源的安全义务。

19.中标方驻场人员应在重要活动、会议期间，根据采购人安全保障要求，参与重保值班值守工作。

20.中标方应按照采购人业务要求，围绕项目内容，提供采购人所需要的业务相关进展及数据，最迟须在采购人要求的24小时内提供准确的信息。

21.中标方在项目中所建设、运营的应用系统、应用服务等涉及鉴权登录的，应使用浙政钉/浙里办扫码方式，若使用账号口令方式的，需要经采购人允许后，并且采用二次验证的方式。

22.中标方驻场人员原则上需按照采购人要求，从事项目中约定的相关驻场工作，不得参与其他项目，不得从事项目中已单独支付服务费的等非驻场工作。

二、安全部分违约责任

1.由于中标方原因，受到国家级安全问题通报的、或造成特别重大事故的，每通报一个问题或发生一次事故，从合同金额内扣除10万元。

2.由于中标方原因，受到省级安全问题通报的、或造成重大事故的，每通报一个问题或发生一次事故，从合同金额扣除5万元。

3.由于中标方原因，受到市级安全问题通报的、或造成较大事故（一般事故）的，每通报一个问题或发生一次事故，从合同金额扣除1万元。

4.中标方未按照采购人要求及时处置所属安全事件、隐患的，每发生一次，从合同金额扣除1万元。

5.中标方存在多名（2人及以上）工作人员共用一个操作账户的，或所主管的系统、云资源等账号出现弱口令的（强口令需至少包含数字、大小写字母、特殊字符等，且无明显规律），每出现1次，从合同金额扣除1000元。

6.未经采购人审批允许，中标方不得私开账号、擅自更改权限，不得对项目云资源私开端口，不得利用项目资源进行与该项目无关的工作，不得将政务网和互联网私自打通的。每出现一次，从合同金额中扣除1000元。

7.中标方发现数据安全缺陷、漏洞等风险时，未立即采取补救措施的；或发生数字安全事件时，未立即采取处置措施的；相关情况未第一时间向采购人报告的；每出现一次，从合同金额中扣除1万元。

8.若中标方未按需提供日志，或提供的操作记录、安全日志等不完整、存在缺失的，每发现一次，每次从合同金额扣除1万元。

9.中标方拒不配合网络数据安全检查或经检查后拒不进行整改的，每出现一次从合同金额中扣除1万元。

10.项目结束后，中标方未按约删除其在项目过程中获取的数据资料并擅自使用或许可他人使用的，承担项目合同总金额10%的违约责任。

11.中标方未配合采购人对项目涉及的资源、系统等常态化安全漏洞扫描，或未及时修复漏洞的，每出现一次，从合同金额扣除1万元。

12. 中标方未配合采购人完成项目中所建设、运营的应用系统、服务等的网络数据安全检查，并且按要求及时完成检查中发现问题的整改,每出现一次，从合同金额中扣除1万元。

13.中标方未按照采购人相关要求，签订《保密承诺书》，办理入场、离场手续的、未入驻全省ISV系统，出现1人次，每人次从合同金额扣除1万元。

14．中标方派驻的驻场人员未按照采购人工作要求进行出勤的，每出现1人次从合同金额扣除500元。

15.中标方不得擅自将项目中涉及的数据拷贝、转移出指定数据区域外进行开发、调试等，包括不限于中标方公司、第三方公司的服务器等，每出现一次，从合同金额扣除1万元。

16.每次通报后，若中标方未及时提供整改报告的；或未根据通报内容及时进行整改的，每出现一次，从合同金额扣除1万元。

17. 中标方在项目中所承建信息系统的开发、测试环境，出现采购人及项目相关的标识名称，或在项目建成后未及时下架测试环境，每出现一次，从合同金额扣除1万元。

18. 中标方驻场人员在重要活动、会议期间，未按照采购人安全保障要求，参与重保值班值守工作，每出现一人次天，从合同金额扣除1千元。

19. 中标方未按照采购人业务要求，围绕项目内容，未及时提供采购人所需要的业务相关进展及数据，每出现一次，从合同金额扣除1千元。

20. 中标方在项目中所建设、运营的应用系统、应用服务等涉及鉴权登录的，未使用浙政钉/浙里办扫码方式、二次验证的方式的，每发现一次，从合同金额扣除1千元。

21. 中标方驻场人员未按照采购人约定允许，从事其他项目内容、本项目中已额外单独支付服务费的相关工作，采购人有权扣除涉及的驻场人员服务费。

22．中标方应当按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规及规章制度要求开展工作，中标方不履行合同义务或者履行合同义务不符合约定的，应当依照法律及合同约定承担相应责任。

未经采购人同意，中标方私下接入杭州市电子政务外网，一经发现，终止合同并且追究责任。

其它：招标文件第四部分评分办法中评审因素相应的其它要求及第五部分采购合同中相应的其他要求。

**第四部分** **评标办法**

**评标办法前附表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评标标准 | 最高分值 | 主观分/客观分属性 | 投标文件中评标标准相应的商务技术资料目录 \* |
| 1 | **（1）项目整体要求（23分）：**本次服务包含下列三块内容，根据招标文件编制相应整体方案，评标专家根据投标方案进行打分。 | 23 | 主观分 | （一）项目整体要求响应情况 |
| **①互联网出口带宽服务方案：** |
| 详细阐述政务外网互联网带宽如何与现有负载设备对接方案，包含①物理端口部署方案、②虚拟端口部署方案及③带宽分配方案。每一项满足得1分，部分满足得0.5分，不满足不得分，共3分（3分）。 |
| **②市民中心设备租赁服务方案：** |
| a、投标人需详细阐述杭州市电子政务外网现有网络情况、设备物理环境、政务网物理光纤链路情况，提供网络系统架构图，并详细阐述割接升级方案的重点及难点，确保系统整体可用性和可靠性。满足得5分，部分满足得2.5分，不满足不得分（5分）。 |
| b、投标人需对政务外网运维平台的工单服务台，自定义流程，自定义表单，IP地址管理方案做详细阐述，并附功能截图。满足得5分，部分满足得2.5分，不满足不得分（5分）。 |
| c、详细阐述本次服务的安全设备部署的如何与现有政务网无缝衔接，提供安全系统架构图。满足得4分，部分满足得2分，不满足不得分（4分）。 |
| d、详细阐述市民中心核心机房系统情况，包括①空调、②UPS、③机柜的布置图、④详细配电系统图纸。每一项满足得1分，部分满足得0.5分，不满足不得分。共4分（4分）。 |
| **③现有设备维保方案**。包括（1）政务外网现有线路基本情况及主备网线路冗余方案；（2）线路及设备巡检模式及巡检方案；（3）现有设备基本情况及整体维保方案；（4）重保及应急方案；根据提供的方案内容进行评分，每一项方案内容完整且合理、可行、满足需求的得 0.5 分，不满足的不得分，共2分（2分）。 |
| 2 | **（2）下列服务内容满足情况（36分）：** | 36 | 客观分 | （二）四大类服务内容满足情况 |
| **●线路资源租赁服务要求满足情况（6分）：** |
| 包含①互联网出口带宽≥8.3G；②政务网相关链路租用须不少于147条；③统一运维服务满足情况；每一项满足得2分，不满足不得分，最高得6分（6分）。 |
| **●设备租赁服务要求满足情况（26分）：** |
| 关于网络、安全设备租赁服务，政务外网运维平台租赁服务，市民中心机房设备租赁服务技术要求，投标人需根据招标文件要求提供点对点应答，对参数不满足或缺失的每一项扣1分，带有✰的参数不满足或缺失每一项扣2分，共26分，扣完为止（26分）。 |
| **●关于现有设备维保服务求满足情况（4分）：** |
| 涉及内容包括：市民中心路由交换设备维保服务、市民中心机房设备（具体见附表）服务，根据要求编制投标文件，投标人需根据招标文件要求提供点对点应答，对参数不满足或缺失的每一项扣1分，带有✰的参数不满足或缺失每一项扣2分，共4分，扣完为止（4分）。 |
| 3 | **（3）售后服务方案情况（14分）：** | 14 | 主观分 | （三）售后服务方案情况 |
| ●满足采购人提出的服务要求，包括①建立针对本项目建立服务保障体系；②提供设备（系统）软件更新、升级、维护、检测、排障；③提供设备（系统）硬件故障检测、排障，备件免费更换；④能提供快速的售后服务响应，故障在15分钟内响应，30分钟到现场，2小时以内解决问题；不能当场修复的，必须采取提供备品、备件或备机等措施以上情况需提供证明材料；⑤提供设备巡检服务；⑥在维保服务过程中，要求向采购人提供网络优化及支持服务；⑦承诺在项目过程中提交满足要求的维护文档。每一项满足得2分，部分满足得1分，不满足不得分。总计14分（14分）。 |
| 4 | **（4）项目组人员素质情况（16分）：** | 16 | 客观分 | （四）项目组人员素质情况 |
| ●项目经理具有信息系统项目管理师证书、网络工程师证书，全部具备得3分，每缺一项扣1.5分。（需提供证书复印件作为凭证）（3分）。 |
| ●拟派技术负责人须具有系统架构设计师（高级）、系统分析师（高级）、信息系统项目管理师（高级）证书，全部具备得3分，每缺一项扣1分。（需提供证书复印件作为凭证）（3分）。 |
| ●服务人员需具备相应的资质，投标人拟派团队其他人员中（项目经理和项目技术负责人2人除外）具备网络工程师证的人员不少于4人，得2分；否则不得分（2分）。 |
| ●驻场网络支持工程师要求：①要求有大专以上学历，1年以上网络设计、建设、管理、维护工作经验，②要求在采购人驻所5×8驻场工作，工作日接受采购人日常考勤和工作任务分配（包括提供相关文档、资料整理、日常管理、系统配置、故障诊断、故障排除等），③应急（或故障）情况下、采购人网络调整（或升级）时，能在非工作时间接受采购人指令工作，并在采购人认为必要时在非工作时间到达设备现场工作，且能做到及时响应和有效处置；④承诺驻场网络支持工程师要求满足95％以上出勤率（到位率）满足一项得2分，不满足不得分，总计8分（8分）。 |
| 5 | **（5）投标人类似项目建设的成功经验（1分）：**投标截止时间前三年内，投标人承担类似项目实施的经验情况。依照投标人提供的合同、合格的用户验收报告。只提供合同的案例（以合同签订时间为准），每个得0.25分，最高得0.5分；同时提供合同和合格的用户验收报告的案例（以验收报告时间为准），每个得0.5分，最高得1分。同一业绩不重复计分，本项最高得1分。 | 1 | 客观分 | （五）类似项目建设的经验情况 |
| 6 | （6）有效投标报价的最低价作为评标基准价，其最低报价为满分；按［投标报价得分=（评标基准价/投标报价）\*最高分值］的计算公式计算。  评标过程中，不得去掉报价中的最高报价和最低报价。  对于未预留份额专门面向中小企业的政府采购服务项目，以及预留份额政府采购服务项目中的非预留部分标项，对小型和微型企业的投标报价给予10%的扣除，用扣除后的价格参与评审。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政府采购服务项目，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，对联合体或者大中型企业的报价给予4%的扣除，用扣除后的价格参加评审。 | 10 |  | / |

 \***备注：**投标人编制投标文件（商务技术文件部分）时，建议按此目录（序号和内容）提供评标标准相应的商务技术资料。

**一、评标方法**

**1.本项目采用综合评分法。**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、评标标准**

**2.** **评标标准：**见评标办法前附表。

**三、评标程序**

**3.1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。不满足招标文件的实质性要求的，投标无效。

**3.2 比较与评价。**评标委员会应当按照招标文件中规定的评标方法和标准，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。

**3.3汇总商务技术得分。**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，并汇总商务技术得分情况。

**3.4报价评审。**

3.4.1投标文件报价出现前后不一致的，按照下列规定修正：

3.4.1.1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;

3.4.1.2大写金额和小写金额不一致的，以大写金额为准;

3.4.1.3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;

3.4.1.4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。

3.4.1.5同时出现两种以上不一致的，按照3.4.1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。

3.4.2投标文件出现不是唯一的、有选择性投标报价的，投标无效。

3.4.3投标报价超过招标文件中规定的预算金额或者最高限价的，投标无效。

3.4.4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。

3.4.5对于未预留份额专门面向中小企业的政府采购服务项目，以及预留份额政府采购服务项目中的非预留部分标项，对小型和微型企业的投标报价给予10%-20%的扣除，用扣除后的价格参与评审。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政府采购服务项目，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，对联合体或者大中型企业的报价给予4%-6%的扣除，用扣除后的价格参加评审。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。

**3.5排序与推荐。**采用综合评分法的，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。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排名第一的中标候选人。

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。

**3.6编写评标报告。**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。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。

**四、评标中的其他事项**

**4.1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需要投标人作出必要的澄清、说明或者补正的，评标委员会和投标人通过电子交易平台交换数据电文，投标人提交使用电子签名的相关数据电文或通过平台上传加盖公章的扫描件。给予投标人提交澄清、说明或补正的时间不得少于半小时，投标人已经明确表示澄清说明或补正完毕的除外。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。

**4.2投标无效。**有下列情形之一的，投标无效：

4.2.1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文件的，视为投标人不具备招标文件中规定的资格要求）；

4.2.2投标文件未按照招标文件要求签署、盖章的；

4.2.3采购人拟采购的产品属于政府强制采购的节能产品品目清单范围的，投标人相应的投标产品未获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书的；

4.2.4投标文件含有采购人不能接受的附加条件的；

4.2.5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；

4.2.6投标文件出现不是唯一的、有选择性投标报价的;

4.2.7投标报价超过招标文件中规定的预算金额或者最高限价的; 投标报价低于项目预算50%，未在报价文件中详细阐述不影响产品质量或者诚信履约的具体原因的；

4.2.8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；

4.2.9投标人对根据修正原则修正后的报价不确认的；

4.2.10投标人提供虚假材料投标的；

4.2.11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；

4.2.12投标人仅提交备份投标文件，未在电子交易平台传输递交投标文件的，投标无效；

4.2.13投标人未提供样品或提供的样品不满足采购需求实质性条件的，投标无效；

## 4.2.14 投标文件不满足招标文件的其它实质性要求的；

4.2.15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。

**5.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：

5.1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；

5.2出现影响采购公正的违法、违规行为的；

5.3投标人的报价均超过了采购预算，采购人不能支付的；

5.4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。

**6.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。

**7.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结果的，依照下列规定处理：

7.1未确定中标供应商的，终止本次政府采购活动，重新开展政府采购活动。

7.2已确定中标供应商但尚未签订政府采购合同的，中标结果无效，从合格的中标候选人中另行确定中标供应商；没有合格的中标候选人的，重新开展政府采购活动。

7.3政府采购合同已签订但尚未履行的，撤销合同，从合格的中标候选人中另行确定中标供应商；没有合格的中标候选人的，重新开展政府采购活动。

7.4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。

7.5政府采购当事人有其他违反政府采购法或者政府采购法实施条例等法律法规规定的行为，经改正后仍然影响或者可能影响中标结果或者依法被认定为中标无效的，依照7.1-7.4规定处理。

**第五部分 拟签订的合同文本**

合同编号：

**政府采购合同参考范本**

**（服务类）**

**第一部分 合同书**

项目名称：

甲方：

乙方：

签订地：

签订日期： 年 月 日

年 月 日， 杭州市数据资源管理局 以 （政府采购方式） 对 杭州市智慧电子政务外网（2024）项目HZZFCG-2024-081 项目进行了采购。经 （相关评定主体名称） 评定， （中标或者成交供应商名称） 为该项目中标或者成交供应商。现于中标或者成交通知书发出之日起10个工作日内，按照采购文件确定的事项签订本合同。

根据《中华人民共和国民法典》《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平和诚实信用的原则，经 杭州市数据资源管理局 (以下简称：甲方)和 （中标或者成交供应商名称） (以下简称：乙方)协商一致，约定以下合同条款，以兹共同遵守、全面履行。

**1.1 合同组成部分**

下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定的事项的前提下，组成本合同的多个文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 中标或者成交通知书；

1.1.3 投标或者响应文件（含澄清或者说明文件）；

1.1.4 采购文件（含澄清或者修改文件）；

1.1.5 其他相关采购文件。

**1.2 标的**

1.2.1 服务内容： ；

1.2.2 服务标准： ；

1.2.3 技术保障：　　　　　　　　　 　 ；

1.2.4 服务人员组成：　　 　 ；

1.2.5合同 （是/否）涉及货物。若涉及货物的，则：

1.2.5.1 货物名称、品牌、规格型号、花色： ；

1.2.5.2 货物数量： ；

1.2.5.3 货物质量：　　　　　　　　　 　 ；

**1.3 价款**

本项目采用以下第 ***合同专用条款*** 条款规定的计价方式计价。

1.3.1总价合同，本合同总价（含税）为：￥ 元（大写： 元人民币）。

分项价格：

|  |  |  |
| --- | --- | --- |
| 序号 | 分项名称 | 分项价格 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 总价 | |  |

1.3.2单价合同，本合同单价（含税）标准为： 。服务工作量的计量方式为： ***合同专用条款*** 。单价合同，在合同履行期间内，根据实际完成的工作量据实结算，但结算总价上限不得超过预算金额或者双方确定的金额￥ 元（大写： 元人民币）。

1.3.3其他计价方式： 。

**1.4履约保证金**

乙方 ***合同专用条款*** （是/否）需要支付履约保证金。若需要支付履约保证金的，则：

1.4.1履约保证金的比例为合同金额的 ***合同专用条款*** %；

1.4.2履约保证金支付方式详见 ***合同专用条款*** ；

## 1.4.3 如果乙方不履行合同，履约保证金不予退还；如果乙方未能按合同约定全面履行义务，那么甲方有权从履约保证金中取得补偿或赔偿，同时不影响甲方要求乙方承担合同约定的超过履约保证金的违约责任的权利；

1.4.4甲方在项目验收结束后及时退还履约保证金。甲方在项目通过验收之日起5 个工作日内将履约保证金无息退还乙方，逾期退还的，乙方可要求甲方支付违约金，违约金按每迟延退还一日的应退还而未退还金额的 0.05 %计算，最高限额为本合同履约保证金的 20 %。

**1.5预付款**

甲方 ***合同专用条款*** （是/否）需要支付预付款。若需要支付预付款的，则：

1.5.1预付款比例、支付方式、时间详见 ***合同专用条款*** ；

1.5.2预付款的扣回方式详见 ***合同专用条款*** ；

1.5.3预付款的担保措施详见 ***合同专用条款*** 。

**1.6资金支付**

1.6.1甲方应严格履行合同，及时组织验收，验收合格后及时将合同款支付完毕。对于满足合同约定支付条件的，甲方自收到发票后5个工作日内将资金支付到合同约定的乙方账户，有条件的甲方可以即时支付。甲方不得以机构变动、人员更替、政策调整、单位放假等为由延迟付款。

1.6.2资金支付的方式、时间和条件详见***合同专用条款***。

**1.7 履行期限、地点和方式**

1.7.1 服务交付（实施）的时间（期限）：***合同专用条款***；

1.7.2 服务交付（实施）的地点（地域范围）：***合同专用条款***；

1.7.3 服务交付（实施）的方式：***合同专用条款***。

1.7.4若服务涉及货物的，则货物的：

1.7.4.1 交付期限：详见***合同专用条款***；

1.7.4.2 交付地点：***合同专用条款***；

1.7.4.3 交付方式：***合同专用条款***。

**1.8违约责任**

1.8.1 除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式交付服务成果或者实施服务，那么甲方可要求乙方支付违约金，迟延履行违约金按每迟延履行一日的应提供而未提供服务价格的0.05 %计算，最高限额为本合同总价的 20 %；迟延履行的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

## 1.8.2服务中涉及的货物，除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式交付货物，那么甲方可要求乙方支付违约金，违约金按每迟延交付货物一日的应交付而未交付货物价格的 0.05 %计算，最高限额为本合同总价的 20 %；迟延交付货物的违约金计算数额达到前述最高限额之日起，甲方有权在要求乙方支付违约金的同时，书面通知乙方解除本合同；

1.8.3除不可抗力外，如果甲方没有按照本合同约定的付款方式付款，那么乙方可要求甲方支付违约金，违约金按每迟延付款一日的应付而未付款的 0.05 %计算，最高限额为本合同总价的 20 %；迟延付款的违约金计算数额达到前述最高限额之日起，乙方有权在要求甲方支付违约金的同时，书面通知甲方解除本合同；

1.8.4 除不可抗力外，任何一方未能履行本合同约定的其他主要义务，经催告后在合理期限内仍未履行的，或者任何一方有其他违约行为致使不能实现合同目的的，或者任何一方有腐败行为（即：提供或给予或接受或索取任何财物或其他好处或者采取其他不正当手段影响对方当事人在合同签订、履行过程中的行为）或者欺诈行为（即：以谎报事实或者隐瞒真相的方法来影响对方当事人在合同签订、履行过程中的行为）的，对方当事人可以书面通知违约方解除本合同；

1.8.5 除前述约定外，任何一方未能履行本合同约定的义务，对方当事人均有权要求继续履行、采取补救措施或者赔偿损失等，且对方当事人行使的任何权利救济方式均不视为其放弃了其他法定或者约定的权利救济方式；

1.8.6如果出现政府采购监督管理部门在处理投诉事项期间，书面通知甲方暂停采购活动的情形，或者询问或质疑事项可能影响中标或者成交结果的，导致甲方中止履行合同的情形，均不视为甲方违约。

1.8.7违约责任***合同专用条款***另有约定的，从其约定。

**1.9合同争议的解决**

本合同履行过程中发生的任何争议，双方当事人均可通过和解或者调解解决；不愿和解、调解或者和解、调解不成的，可以选择以下第 ***合同专用条款*** 条款规定的方式解决：

1.9.1 将争议提交***合同专用条款***仲裁委员会依申请仲裁时其现行有效的仲裁规则裁决；

1.9.2 向***合同专用条款***人民法院起诉。

**1.10 合同生效**

本合同自双方当事人盖章签字时生效。

**甲方**：  **乙方**：

统一社会信用代码： 统一社会信用代码或身份证号码：

住所： 住所：

法定代表人或 法定代表人或

授权代表（签字）： 授权代表（签字）:

联系人： 联系人：

约定送达地址： 约定送达地址：

邮政编码： 邮政编码：

电话: 电话:

传真: 传真:

电子邮箱： 电子邮箱：

开户银行： 开户银行：

开户名称： 开户名称：

开户账号： 开户账号：

**第二部分 合同一般条款**

**2.1 定义**

本合同中的下列词语应按以下内容进行解释：

2.1.1 “合同”系指采购人和中标或成交供应商签订的载明双方当事人所达成的协议，并包括所有的附件、附录和构成合同的其他文件。

2.1.2 “合同价”系指根据合同约定，中标或成交供应商在完全履行合同义务后，采购人应支付给中标或成交供应商的价格。

2.1.3 “服务”系指中标或成交供应商根据合同约定应向采购人履行的除货物和工程以外的其他政府采购对象，包括采购人自身需要的服务和向社会公众提供的公共服务。

2.1.4 “甲方”系指与中标或成交供应商签署合同的采购人；采购人委托采购代理机构代表其与乙方签订合同的，采购人的授权委托书作为合同附件。

2.1.5 “乙方”系指根据合同约定提供服务的中标或成交供应商；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的，联合体各方均应为乙方或者与乙方相同地位的合同当事人，并就合同约定的事项对甲方承担连带责任。

2.1.6 “现场”系指合同约定提供服务的地点。

**2.2 技术规范**

服务所应遵守的技术规范应与采购文件规定的技术规范和技术规范附件(如果有的话)及其技术规范偏差表(如果被甲方接受的话)相一致；如果采购文件中没有技术规范的相应说明，那么应以国家有关部门最新颁布的相应标准和规范为准。

**2.3 知识产权**

2.3.1 乙方应保证其提供的服务不受任何第三方提出的侵犯其著作权、商标权、专利权等知识产权方面的起诉；如果任何第三方提出侵权指控，那么乙方须与该第三方交涉并承担由此发生的一切责任、费用和赔偿，乙方还应及时澄清相关信息，使甲方声誉免受损害，甲方保留追责的权利。

2.3.2 合同涉及技术成果的归属和收益的分成办法的，详见***合同专用条款***。

**2.4 履约检查和问题反馈**

2.4.1甲方有权在其认为必要时，对乙方是否能够按照合同约定提供服务进行履约检查，以确保乙方所提供的服务能够依约满足甲方之项目需求，但不得因履约检查妨碍乙方的正常工作，乙方应予积极配合；

2.4.2 合同履行期间，甲方有权将履行过程中出现的问题反馈给乙方，双方当事人应以书面形式约定需要完善和改进的内容。

**2.5 结算方式和付款条件**

详见***合同专用条款***。

**2.6 技术资料和保密义务**

2.6.1 乙方有权依据合同约定和项目需要，向甲方了解有关情况，调阅有关资料等，甲方应予积极配合；

2.6.2 乙方有义务妥善保管和保护由甲方提供的前款信息和资料等；

2.6.3 除非依照法律规定或者对方当事人的书面同意，任何一方均应保证不向任何第三方提供或披露有关合同的或者履行合同过程中知悉的对方当事人任何未公开的信息和资料，包括但不限于技术情报、技术资料、商业秘密和商业信息等，并采取一切合理和必要措施和方式防止任何第三方接触到对方当事人的上述保密信息和资料。

**2.7 质量保证**

2.7.1 乙方应建立和完善履行合同的内部质量保证体系，并提供相关内部规章制度给甲方，以便甲方进行监督检查；

2.7.2 乙方应保证履行合同的人员数量和素质、软件和硬件设备的配置、场地、环境和设施等满足全面履行合同的要求，并应接受甲方的监督检查。

**2.8 延迟履行**

甲乙双方签订合同后，乙方应按照合同约定履行合同义务，除不可抗力外，乙方不得延迟履行。在合同履行过程中，如果因不可抗力，乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时提供服务的理由、预期延误时间通知甲方；甲方收到乙方通知后，认为其理由正当的，可以书面形式酌情同意乙方可以延长履行的具体时间。

**2.9 合同变更**

合同继续履行将损害国家利益和社会公共利益的，双方当事人应当以书面形式变更合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

**2.10 合同转让和分包**

合同的权利义务依法不得转让，但经甲方书面同意，乙方可以依法采取分包方式履行合同，即：依法可以将合同项下的部分非主体、非关键性工作分包给他人完成，接受分包的人应当具备相应的资格条件，并不得再次分包，且乙方应就分包项目向甲方负责，并与分包供应商就分包项目向甲方承担连带责任。

**2.11 不可抗力**

2.11.1如果任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间；

2.11.2 因不可抗力致使不能实现合同目的的，当事人可以解除合同；

2.11.3 因不可抗力致使合同有变更必要的，双方当事人应在***合同专用条款***约定时间内以书面形式变更合同；

2.11.4受不可抗力影响的一方在不可抗力发生后，应在***合同专用条款***约定时间内以书面形式通知对方当事人，并在***合同专用条款***约定时间内，将有关部门出具的证明文件送达对方当事人。

**2.12 税费**

与合同有关的一切税费，均按照中华人民共和国法律的相关规定缴纳。

**2.13 乙方破产**

如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方终止合同且不给予乙方任何补偿和赔偿，但合同的终止不损害或不影响甲方已经采取或将要采取的任何要求乙方支付违约金、赔偿损失等的行动或补救措施的权利。

**2.14 合同中止、终止**

2.14.1 双方当事人不得擅自中止或者终止合同；

2.14.2合同继续履行将损害国家利益和社会公共利益的，双方当事人应当中止或者终止合同。有过错的一方应当承担赔偿责任，双方当事人都有过错的，各自承担相应的责任。

**2.15 检验和验收**

2.15.1 乙方按照***合同专用条款***的约定，定期提交服务报告，甲方按照***合同专用条款***的约定进行定期验收；

2.15.2 合同期满或者履行完毕后，甲方有权组织（包括依法邀请国家认可的质量检测机构参加）对乙方履约的验收，即：按照合同约定的标准，组织对乙方履约情况的验收，并出具验收书；向社会公众提供的公共服务项目，验收时应当邀请服务对象参与并出具意见，验收结果应当向社会公告；

2.15.3 检验和验收标准、程序等具体内容以及前述验收书的效力详见***合同专用条款****。*

**2.16 通知和送达**

2.17.1任何一方因履行合同而以合同第一部分尾部所列明的传真或电子邮件 发出的所有通知、文件、材料，均视为已向对方当事人送达；任何一方变更上述送达方式或者地址的，应于3个工作日内书面通知对方当事人，在对方当事人收到有关变更通知之前，变更前的约定送达方式或者地址仍视为有效。

2.17.2以当面交付方式送达的，交付之时视为送达；以电子邮件方式送达的，发出电子邮件之时视为送达；以传真方式送达的，发出传真之时视为送达；以邮寄方式送达的，邮件挂号寄出或者交邮之日之次日视为送达。

**2.17 合同使用的文字和适用的法律**

2.17.1 合同使用汉语书就、变更和解释；

2.17.2 合同适用中华人民共和国法律。

**2.18 计量单位**

除技术规范中另有规定外,合同的计量单位均使用国家法定计量单位。

**2.19合同份数**

合同份数按***合同专用条款***规定，每份均具有同等法律效力。

**第三部分 合同专用条款**

本部分是对前两部分的补充和修改，如果前两部分和本部分的约定不一致，应以本部分的约定为准。本部分的条款号应与前两部分的条款号保持对应；与前两部分无对应关系的内容可另行编制条款号。

|  |  |
| --- | --- |
| **条款号** | **约定内容** |
| 1.3 | 本项目采用以下第 1 条款规定的计价方式计价。 |
| 1.3.1 | 本次项目合同金额为大写人民币 整（￥ 元），采用分期付款方式，具体如下：  第一期付款：合同签订后，甲方在5个工作日内支付项目合同金额的45%，计人民币 整（￥ 元）。  第二期付款：完成项目阶段性验收后，甲方收到乙方提供的增值税普通发票后5个工作日内支付项目合同金额的20%，计人民币 整（￥ 元）。  第三期付款：完成项目终验后，甲方收到乙方提供的增值税普通发票后5个工作日支付项目合同金额的35%，计人民币 整（￥ 元）。  甲方无故逾期支付服务费用的，按照每逾期一日支付本期应支付服务费额度的5‰承担违约责任。 |
| 1.4 | 乙方 否 （是/否）需要支付履约保证金。 |
| 1.4.1 | 履约保证金的比例为合同金额的 / %； |
| 1.4.2 | / |
| 1.5 | 甲方 否 （是/否）需要支付预付款。 |
| 1.5.1 | / |
| 1.5.2 | / |
| 1.5.3 | / |
| 1.6.2 | 本次项目合同金额为大写人民币 整（￥ 元），采用分期付款方式，具体如下：  第一期付款：合同签订后，甲方收到乙方提供的增值税普通发票确认无误后5个工作日内支付项目合同金额的45%，计人民币 整（￥ 元）。  第二期付款：完成项目阶段性验收，甲方收到乙方提供的增值税普通发票后确认无误后5个工作日内支付项目合同金额的20%，计人民币 整（￥ 元）。  第三期付款：完成项目终验后，甲方收到乙方提供的增值税普通发票确认无误后5个工作日支付项目合同金额的35%，计人民币 整（￥ 元）。  甲方无故逾期支付服务费用的，按照每逾期一日支付本期应支付服务费额度的5‰承担违约责任。 |
| 1.7.1 | 2024.7.1-2025.6.30 |
| 1.7.2 | 甲方指定 |
| 1.7.3 | 甲方指定 |
| 1.7.4.1 | / |
| 1.7.4.2 | / |
| 1.7.4.3 | / |
| 1.8.7 | / |
| 1.9 | 当地法院起诉 |
| 1.9.1 | 杭州市 |
| 1.9.2 | 杭州市 |
| 2.3.2 | 归甲方所有 |
| 2.5 | 本次项目合同金额为大写人民币 整（￥ 元），采用分期付款方式，具体如下：  第一期付款：合同签订后，甲方在5个工作日内支付项目合同金额的45%，计人民币 整（￥ 元）。  第二期付款：完成项目阶段性验收后，甲方收到乙方提供的增值税普通发票后5个工作日内支付项目合同金额的20%，计人民币 整（￥ 元）。  第三期付款：完成项目终验后，甲方收到乙方提供的增值税普通发票后5个工作日支付项目合同金额的35%，计人民币 整（￥ 元）。  甲方无故逾期支付服务费用的，按照每逾期一日支付本期应支付服务费额度的5‰承担违约责任。 |
| 2.11.3 | 提前一个月 |
| 2.11.4 | 提前一个月 |
| 2.15.1 | 提前 |
| 2.15.3 | 招标要求 |
| 2.19 | 合同份数陆份，甲乙各执叁份，每份均具有同等法律效力 |

**第六部分 应提交的有关格式范例**

**资格文件部分**

**目录**

（1）符合参加政府采购活动应当具备的一般条件的承诺函……………（页码）

（2）联合协议………………………………………………………………（页码）

（3）落实政府采购政策需满足的资格要求………………………………（页码）

（4）本项目的特定资格要求………………………………………………（页码）

**一、 符合参加政府采购活动应当具备的一般条件的承诺函**

杭州市数据资源管理局、杭州市公共资源交易中心：

我方参与杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】政府采购活动，郑重承诺：

（一）具备《中华人民共和国政府采购法》第二十二条第一款规定的条件：

1、具有独立承担民事责任的能力；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必需的设备和专业技术能力；

4、有依法缴纳税收和社会保障资金的良好记录；

5、参加政府采购活动前三年内，在经营活动中没有重大违法记录；

6、具有法律、行政法规规定的其他条件。

（二）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。

（三）不存在以下情况：

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；

2、为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后再参加该采购项目的其他采购活动的。

投标人名称(电子签名)：

日期： 年 月 日

注：根据《关于规范政府采购供应商资格设定及资格审查的通知》（浙财采监[2013]24号）的相关规定，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，参与政府采购活动，如果已经依法办理了工商、税务和社保登记手续，**除提供上述《符合参加政府采购活动应当具备的一般条件的承诺函》外，还需提供下列材料：总公司（总机构）的授权书或提供房产权证或其他有效财产证明材料，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。**

**二、联合协议（如果有）**

**[以联合体形式投标的，提供联合协议（附件5）；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）]**

**三、落实政府采购政策需满足的资格要求（如果有）**

（根据招标公告落实政府采购政策需满足的资格要求选择提供相应的材料；未要求的，无需提供）

**A**.专门面向中小企业，服务全部由符合政策要求的中小企业（或小微企业）承接的，提供相应的中小企业声明函（附件7）。

**B.**要求以联合体形式参加的，提供联合协议（附件5）和中小企业声明函（附件7），联合协议中中小企业合同金额应当达到招标公告载明的比例；如果供应商本身提供所有标的均由中小企业承接的，并相应达到了前述比例要求，视同符合了资格条件，无需再与其他中小企业组成联合体参加政府采购活动，无需提供联合协议。

**C、**要求合同分包的，提供分包意向协议（附件6）和中小企业声明函（附件7），分包意向协议中中小企业合同金额应当达到招标公告载明的比例；如果供应商本身提供所有标的均由中小企业承接的，并相应达到了前述比例要求，视同符合了资格条件，无需再向中小企业分包，无需提供分包意向协议。

**四、本项目的特定资格要求（如果有）**

（根据招标公告本项目的特定资格要求提供相应的材料；未要求的，无需提供）

**商务技术文件部分**

**目录**

（1）投标函…………………………………………………………………………………（页码）（2）授权委托书或法定代表人（单位负责人、自然人本人）身份证明………（页码）

（3）分包意向协议…………………………………………………………………………（页码）

（4）符合性审查资料………………………………………………………………………（页码）

（5）评标标准相应的商务技术资料……………………………………………………（页码）（6）投标标的清单……………………………………………………………………（页码）（7）商务技术偏离表………………………………………………………………………（页码）

（8）政府采购供应商廉洁自律承诺书…………………………………………………（页码）

**一、投标函**

杭州市数据资源管理局、杭州市公共资源交易中心：

我方参加你方组织的杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】招标的有关活动，并对此项目进行投标。为此：

1、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90天），本投标文件在投标有效期满之前均具有约束力。

2、我方的投标文件包括以下内容：

2.1资格文件：

2.1.1承诺函；

2.1.2联合协议（如果有)；

2.1.3落实政府采购政策需满足的资格要求（如果有）；

2.1.4本项目的特定资格要求（如果有)。

2.2 商务技术文件：

2.2.1投标函；

2.2.2授权委托书或法定代表人（单位负责人）身份证明；

2.2.3分包意向协议（如果有)；

2.2.4符合性审查资料；

2.2.5评标标准相应的商务技术资料；

2.2.6投标标的清单；

2.2.7商务技术偏离表；

2.2.8政府采购供应商廉洁自律承诺书；

2.3报价文件

2.3.1开标一览表（报价表）；

2.3.2 报价情况说明（如果有）；

2.3.3中小企业声明函（如果有）。

3、我方承诺除商务技术偏离表列出的偏离外，我方响应招标文件的全部要求。对投标文件中材料的真实性、合法性负责。

4、如我方中标，我方承诺：

4.1在收到中标通知书后，在中标通知书规定的期限内与你方签订合同；

4.2在签订合同时不向你方提出附加条件；

4.3按照招标文件要求提交履约保证金；

4.4在合同约定的期限内完成合同规定的全部义务。

5、其他补充说明: 。

投标人名称（电子签名）：

日期： 年 月 日

注：按本格式和要求提供。

**二、授权委托书或法定代表人（单位负责人、自然人本人）身份证明**

**授权委托书（适用于非联合体投标）**

杭州市数据资源管理局、杭州市公共资源交易中心：

现委托 （姓名）为我方代理人（身份证号码： ，手机： ，所在单位： ），以我方名义处理杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】政府采购投标的一切事项，其法律后果由我方承担。

委托期限：自 年 月 日起至 年 月 日止。

特此告知。

投标人名称(电子签名)：

签发日期： 年 月 日

**授权委托书（适用于联合体投标）**

杭州市数据资源管理局、杭州市公共资源交易中心：

现委托 （姓名）为我方代理人（身份证号码： ，手机： ，所在单位： ），以我方名义处理杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】政府采购投标的一切事项，其法律后果由我方承担。

委托期限：自 年 月 日起至 年 月 日止。

特此告知。

联合体成员名称(电子签名/公章)：

联合体成员名称(电子签名/公章)：

……

日期： 年 月 日

注：▲供应商委派不在本单位缴纳社保的人员作为授权代表（代理人）的，应当在投标（响应）文件中，说明具体原因、授权代表缴纳社保的单位，并附列该授权代表缴纳社保清单。

**法定代表人、单位负责人或自然人本人的身份证明（适用于法定代表人、单位负责人或者自然人本人代表投标人参加投标）**

身份证件扫描件：

|  |
| --- |
| 正面： 反面： |

投标人名称(电子签名)：

日期： 年 月 日

**三、分包意向协议（如果有）**

[**中标后以分包方式履行合同的，提供分包意向协议(附件6)；采购人不同意分包或者投标人中标后不以分包方式履行合同的，则不需要提供。**]

**四、符合性审查资料**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **实质性要求** | **需要提供的符合性审查资料** | **投标文件中的**  **页码位置** |
| 1 | 投标文件按照招标文件要求签署、盖章。 | 需要使用电子签名或者签字盖章的投标文件的组成部分 | 见投标文件  第 页 |
| 2 | 投标文件中承诺的投标有效期不少于招标文件中载明的投标有效期。 | 投标函 | 见投标文件第 页 |
| 3 | 投标文件满足招标文件的其它实质性要求。 | 招标文件其它实质性要求相应的材料（“▲” 系指实质性要求条款，招标文件无其它实质性要求的，无需提供） | 见投标文件第 页 |

注：按本格式和要求提供。

**五、评标标准相应的商务技术资料**

**（按招标文件第四部分评标办法前附表中“投标文件中评标标准相应的商务技术资料目录”提供资料。）**

**六、投标标的清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **服务范围** | **服务要求** | **服务时间** | **服务标准** | **备注（如果有）** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| …… |  |  |  |  |  |  |

注：按本格式和要求提供。

**七、商务技术偏离表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **招标文件章节及具体内容** | **投标文件章节及具体内容** | **偏离说明** |
| 1 |  |  |  |
| 2 |  |  |  |
| …… |  |  |  |

投标人保证：除商务技术偏离表列出的偏离外，投标人响应招标文件的全部要求

注：按本格式和要求提供。

**八、政府采购供应商廉洁自律承诺书**

杭州市数据资源管理局、杭州市公共资源交易中心：

我单位响应你单位项目招标要求参加投标。在这次投标过程中和中标后，我们将严格遵守国家法律法规要求，并郑重承诺：

一、不向项目有关人员及部门赠送礼金礼物、有价证券、回扣以及中介费、介绍费、咨询费等好处费；

二、不为项目有关人员及部门报销应由你方单位或个人支付的费用；

三、不向项目有关人员及部门提供有可能影响公正的宴请和健身娱乐等活动；

四、不为项目有关人员及部门出国（境）、旅游等提供方便；

五、不为项目有关人员个人装修住房、婚丧嫁娶、配偶子女工作安排等提供

好处；

六、严格遵守《中华人民共和国政府采购法》《中华人民共和国招标投标

法》《中华人民共和国民法典》等法律法规，诚实守信，合法经营，坚决抵制各种违法违纪行为。

如违反上述承诺，你单位有权立即取消我单位投标、中标或在建项目的建设资格，有权拒绝我单位在一定时期内进入你单位进行项目建设或其他经营活动，并通报市财政局。由此引起的相应损失均由我单位承担。

投标人名称（电子签名）：

日期： 年 月 日

注：按本格式和要求提供。

**报价文件部分**

**目录**

（1）开标一览表（报价表）………………………………………………………（页码）

（2）报价情况说明…………………………………………………………………（页码）

（3）中小企业声明函………………………………………………………………（页码）

一、开标一览表（报价表）

杭州市数据资源管理局、杭州市公共资源交易中心：

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，我方承诺按照如下开标一览表（报价表）的价格完成杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】的实施。

**开标一览表（报价表）(单位均为人民币元)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **服务范围** | **服务要求** | **服务时间** | **服务标准** | **服务人数** | **备注（如果有）** |
| 1 | XX |  |  |  |  |  |  |
| 2 | XX |  |  |  |  |  |  |
| … |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **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**，否则视为投标文件含有采购人不能接受的附加条件，投标无效；**。

2、有关本项目实施所涉及的一切费用均计入报价。采购人不得向供应商索要或者接受供应商给予的赠品、回扣或者与采购无关的其他商品、服务；如供应商承诺提供赠品、回扣、采购预算中本身不包含的其他商品或服务，视作无效承诺，不得因无效承诺对供应商实行差别待遇或者歧视待遇，也不得将其作为中标（成交）条件或者合同签订条件；总价不为零，报价明细表中部分产品、服务单价为零的，视作已包含在总价中。**采购内容未包含在《开标一览表（报价表）》名称栏中，投标人不能作出合理解释的，视为投标文件含有采购人不能接受的附加条件的，投标无效。**

3、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，主要中标标的名称、服务范围、服务要求、服务时间、服务标准等予以公示。

4、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。

二、报价情况说明（如果有）

（如供应商报价低于项目预算50%的，应当提交本文档，详细阐述不影响产品质量或者诚信履约的具体原因**，否则投标无效。**）

三、中小企业声明函（如果有）

**[招标公告落实政府采购政策需满足的资格要求为“无”即本项目或标项未预留份额专门面向中小企业时，符合《政府采购促进中小企业发展管理办法》规定的小微企业拟享受价格扣除政策的，需提供中小企业声明函（附件7）。]**

# 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，且本单位参加杭州市数据资源管理局单位的杭州市智慧电子政务外网（2024）项目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。

投标人名称（电子签名）：

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：

采购文件获取日期：

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：

代理机构名称：

采购文件公告: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/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。

**附件4：业务专用章使用说明函**

杭州市数据资源管理局、杭州市公共资源交易中心：

我方 (投标人全称)是中华人民共和国依法登记注册的合法企业，在参加你方组织的杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】投标活动中作如下说明：我方所使用的“XX专用章”与法定名称章具有同等的法律效力，对使用“XX专用章”的行为予以完全承认，并愿意承担相应责任。

特此说明。

投标单位（法定名称章）：

日期： 年 月 日

**附：**

投标单位法定名称章（印模） 投标单位“XX专用章”（印模）

**附件5：联合协议**

**（以联合体形式投标的，提供联合协议；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）**

（联合体所有成员名称）自愿组成一个联合体，以一个投标人的身份参加杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】投标。

一、各方一致决定，（某联合体成员名称）为联合体牵头人，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：

（联合体成员1）承担的工作和义务为： ；

（联合体成员2）承担的工作和义务为： ；

……

四、联合体成员中小企业合同份额。

1、（联合体成员X,……）提供的服务由小微企业承接，其合同份额占到合同总金额 %以上。**（****未预留份额专门面向中小企业采购的的采购项目，以及预留份额中的非预留部分采购包，接受联合体投标的，联合协议约定小微企业的合同份额占到合同总金额30%以上的，对联合体报价按评标标准确定的比例给予扣除。供应商拟享受以上价格扣除政策的，填写有关内容。）**

2、中小企业合同金额达到 %，其中小微企业合同金额达到 %。**（要求以联合体形式参加的项目或采购包，供应商按招标文件第一部分招标公告申请人的资格要求中规定的联合协议中中小企业、小微企业合同金额应当达到的比例要求填写。）**

五、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。

六、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。

联合体成员名称(电子签名/公章)：

联合体成员名称(电子签名/公章)：

……

日期： 年 月 日

注：按本格式和要求提供。

**附件6：分包意向协议**

（**中标后以分包方式履行合同的，提供分包意向协议；采购人不同意分包或者投标人中标后不以分包方式履行合同的，则不需要提供。**）

（投标人名称）若成为杭州市智慧电子政务外网（2024）项目【招标编号：HZZFCG-2024-081】的中标供应商，将依法采取分包方式履行合同。（投标人名称）与（所有分包供应商名称）达成分包意向协议。

一、分包标的及数量

（投标人名称）将 XX工作内容 分包给（分包供应商1名称），（分包供应商2名称），具备承担XX工作内容相应资质条件且不得再次分包；

## ……

二、分包供应商中小企业合同份额

1、（分包供应商X,……）提供的服务全部由小微企业承接，其合同份额占到合同总金额 %以上。**（未预留份额专门面向中小企业采购的的采购项目，以及预留份额中的非预留部分采购包，允许分包的，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，对大中型企业的报价按评标标准确定的比例给予扣除。供应商拟享受以上价格扣除政策的，填写有关内容。）**

2、中小企业合同金额达到 %，其中小微企业合同金额达到 %。**（要求合同分包形式参加的项目或采购包，供应商按招标文件第一部分招标公告申请人的资格要求中规定的分包意向协议中中小企业、小微企业合同金额应当达到的比例要求填写。）**

三、分包工作履行期限、地点、方式

四、质量

五、价款或者报酬

六、违约责任

七、争议解决的办法

八、其他

中小企业合同金额达到 %，小微企业合同金额达到 % 。 投标人名称(电子签名)：

分包供应商名称(电子签名/公章)：

……

日期： 年 月 日

注：按本格式和要求提供。

**附件7：中小企业声明函**

**中小企业声明函（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 杭州市数据资源管理局 的 杭州市智慧电子政务外网（2024）项目 采购活动，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. 杭州市智慧电子政务外网（2024）项目，属于 软件和信息技术服务业行业 ；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（电子签名）：

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：

1、填写要求：①“标的名称”、“采购文件中明确的所属行业”依据招标文件第二部分投标人须知前附表中“采购标的及其对应的中小企业划分标准所属行业”的指引逐一填写，不得缺漏；②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；③中型企业、小型企业、微型企业等3种企业类型，结合以上数据，依据《中小企业划型标准规定》（工信部联企业〔2011〕300号）确定；④投标人提供的《中小企业声明函》与实际情况不符的或者未按以上要求填写的，中小企业声明函无效，不享受中小企业扶持政策。声明内容不实的，属于提供虚假材料谋取中标、成交的，依法承担法律责任。

2、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。