杭州市公安业务网安全服务项目

招标文件

**（电子招投标）**

编号:ZHZB-2024HZGA-02

杭州市公安局

浙江正浩招标代理有限公司

二〇二四年四月

**目 录**

第一部分 招标公告

第二部分 投标人须知

第三部分 采购需求

第四部分 评标办法

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

杭州市公安业务网安全服务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4月25日14点00分00秒](https://www.zcygov.cn/）获取（下载）招标文件，并于202%20年%20月%20日%20点%20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：**ZHZB-2024HZGA-02

**项目名称：**杭州市公安业务网安全服务项目

**预算金额：**472万元（其中2024年预算安排250万元）

**采购需求：**杭州市公安业务网安全服务项目，主要工作内容为保证杭州市公安局公安业务网和数据的安全稳定运行，通过采购等保测评服务、数据库审计服务、政务网云日志审计服务、政务网态势感知服务、SaaS化安全服务、公安网安全风险感知服务、公安网桌面云服务、公安网一机两用服务、视频网终端杀毒服务、系统安全检测、网络安全检查、重保、应急响应、边界通道租赁服务，提升杭州市公安局公安业务网网络与数据安全的能力。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：**2024年6月1日至2025年5月31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43% ，小微企业合同金额应当达到28% ;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；

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4月25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4月25日14点00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4月25日14点00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、采购代理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：杭州市公安局

地 址：杭州市华光路35号

项目联系人（询问）：李先生

项目联系方式（询问）：0571-89590197

质疑联系人：陈先生

质疑联系方式：0571-89590205

2.采购代理机构信息

名 称：浙江正浩招标代理有限公司

地 址：杭州市拱墅区祥园路45号盘石全球数字经济产业园D座409室

项目联系人（询问）：方晨

项目联系方式（询问）：18057185267

质疑联系人：杨倩

质疑联系方式：15395821972

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：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：杭州市公安业务网安全服务项目，属于(十二）软件和信息技术服务业行业；  从业人员300人以下或营业收入10000万元以 下的为中小微型企业。其中，从业人员100人及以上，且营业收入1000万元及以上的为中型企业；从业人员10人及以上，且营业收入50万元及以上的为小型企业；从业 人员10人以下或营业收入50万元以下的为微型企业。 |
| 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。 |
| 4 | **分包** | A同意将非主体、非关键性的“等保测评服务、边界通道租赁服务、公安网一机两用服务、公安网桌面云服务”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，  （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：详见评标办法；  （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、采购代理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、采购代理机构不负保管义务；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（编制时可根据项目情况进行调整）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（编制时可根据项目情况进行调整）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 ，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** | 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。 |
| 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：杭州市拱墅区祥园路45号盘石全球数字经济产业园D座409室；备份投标文件签收人员联系电话：方晨；18057185267。**采购人、采购代理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。 |
| 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。  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。 |
| 14 | **采购代理机构代理费用** | 中标人需向浙江正浩招标代理有限公司支付招标代理服务费，收费标准为：以中标通知书中确定的中标总金额作为收费的计算基数，按照《关于杭州市招标代理服务收费管理有关问题的通知》(杭价费[2003]148号)文件规定的相应项目收费标准下浮65%取费。  以上费用由中标人在领取中标通知书时一次性向采购代理机构付清。(开户名：浙江正浩招标代理有限公司,开户银行：浙商银行杭州分行营业部；账号：3310010010120101045391) |

**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 “采购代理机构”系指招标公告中载明的本项目的采购代理机构。

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”系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、采购代理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）》。鼓励采购单位优先采购秸秆环保板材等资源综合利用产品。鼓励采购单位优先采购绿色物流配送服务、提供新能源交通工具的租赁服务。

3.2.4 鼓励供应商在参加政府采购过程中开展绿色设计、选择绿色材料、打造绿色制造工艺、开展绿色运输、做好废弃产品回收处理，实现产品全周期的绿色环保。鼓励采购单位对其提高预付款比例、免收履约保证金。

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。

3.3.4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代理机构提出质疑，否则，采购人或者采购代理机构不予受理：

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采购人或者采购代理机构应当在收到供应商的书面质疑后七个工作日内作出答复，并以书面形式通知质疑供应商和其他与质疑处理结果有利害关系的政府采购当事人，但答复的内容不得涉及商业秘密。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）,采购人或者采购代理机构在质疑回复后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。

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根据政府采购行政裁决省市区三级联动试点工作安排，杭州市本级、拱墅区、富阳区政府采购项目投诉材料可寄送至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、王女士，电话：0571-85252453。

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。

投诉书范本及制作说明详见附件3。

**二、招标文件的构成、澄清、修改**

**5．招标文件的构成**

5.1 招标文件包括下列文件及附件：

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，以书面形式向采购代理机构提出。

6.2 采购代理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。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、采购代理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，采购代理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、采购代理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光盘等存储介质中。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代理机构，采购代理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。采购代理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，采购代理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。

**四、开标、资格审查与信用信息查询**

**18.开标**

18.1采购代理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。采购代理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采购人或采购代理机构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，采购人或采购代理机构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：采购代理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【评标委员会由采购人代表和评审专家组成，成员人数为5人（采购人代表1人，评标专家4人由采购代理机构从政府采购云平台专家库随机抽取产生】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。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，采购代理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。采购代理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代理机构的名称、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。

**23.4** 由于中标、成交供应商原因导致重新采购的，应当承担支付代理费和专家评审费等费用在内的赔偿责任。

**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%，鼓励根据项目特点、供应商诚信等因素免收履约保证金或降低缴纳比例。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**

**28. 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，采购代理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。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。采购人委托第三方成立验收小组。投标人应配合采购人组织的专项验收。验收小组由5人单数组成（1人为采购人代表，其余4名由代理机构在政府采购云平台政企区专家库中随机抽取产生）。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**

**（一）项目概况**

杭州市公安业务网安全服务项目，主要工作内容为保证杭州市公安局公安业务网和数据的安全稳定运行，通过采购等保测评服务、数据库审计服务、政务网云日志审计服务、政务网态势感知服务、SaaS化安全服务、公安网安全风险感知服务、公安网桌面云服务、公安网一机两用服务、视频网终端杀毒服务、系统安全检测、网络安全检查、重保、应急响应、边界通道租赁服务，提升杭州市公安局公安业务网网络与数据安全的能力。

政策依据：

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《关键信息基础设施安全保护条例》

《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》

《GB/T 22240-2020 信息安全技术网络安全等级保护定级指南》

《浙江公安信息网安全管理规定实施细则（试行）》

《关于切实加强公安网终端“一机两用”安全防范工作的通知》

《公安信息通信网边界接入平台安全规范-公网信息采集部分》（公科信[2013] 130号）

1. **预算金额：472万元（其中2024年预算安排250万元）**

**（三）**采购标的是否进口产品： □进口 □国产（本项目为服务类项目）

**（四）**需满足的政府采购政策目标和具体支持对象

□扶持中小企业□节能环保☑其他（本项目预留43%专门面向中小企业，28%专门面向小微企业）

**（五）拟采购标的的服务要求**

|  |  |
| --- | --- |
| 1、等保测评服务：针对采购人的重要信息系统提供等保测评服务。 | |
| 服务内容 | 1、对于测评结论符合等保要求的，出具测评报告及整改建议书。  2、对于测评结论不符合等保要求的，出具差距分析报告及整改建议书。  3、本项目服务期内测评系统数量不少于25个。 |
| 服务要求 | 1、测评依据：须根据国家标准GB/T 22239-2019：《信息安全技术网络安全等级保护基本要求》要求选取安全基础指标开展检测工作，并出具符合国家相关规范要求的测评报告。  2、实施方案：投标人对具体测评系统详细了解的基础上，编制针对性的等级保护测评整体实施方案，包括项目概述、等保测评范围和内容、项目实施流程、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。  3、运行环境：安全测评需要的运行环境（如场地、网络环境等）由采购人提供，投标人应详细描述需要的运行环境的具体要求。  4、项目实施流程：投标人应具有等保工具箱、商用密码检测工具、软件测试工具、代码审计工具。本次等级保护测评实施过程中所使用到的工具软件由投标人推荐，需经采购人确认后方由投标人提供并在测评中使用。供应商应在投标文件中详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。 |
| 交付物 | 《信息系统安全等级保护备案表》（初次测评系统）  《信息系统安全等级保护定级报告》（初次测评系统）  《整体测评实施方案》  《等级保护测评报告》  《等级保护整改建议书》 |
| **2、数据库审计服务：**针对杭州市公安局的政务外网、视频专网和公安网提供数据库审计服务，满足等级保护的合规性需求，同时配合相关人工服务对数据库审计内容进行处理，发现存在的问题及时研判、预警、处理，建立完备安全保障机制。对杭州公安各类安全违规事件进行实时监测、实时预警，协助采购人及时、有效开展整改，切实降低各类安全风险，有效减少部、省、市上级网络安全管理职能部门的各类安全事件通报。配合相关人工服务进行日常运维。 | |
| 服务内容 | 因服务要求，数据库审计服务需提供数据库审计设备。政务网不少于2套（不限制支持的数据库实例个数）、视频专网不少于4台、公安网不少于6台。 |
| 服务要求 | 一、该服务需要提供以下的服务要求支持：  1、模块支持：数据库审计、风险漏洞扫描、状态监控、敏感数据扫描等功能。  2、数据库类型支持：国际主流数据库： Oracle、MySQL、SQLserver、DB2、Sybase、Informix、Teradata、PostgreSQL、Access、cache等；国产数据库：达梦、南大通用、人大金仓、神通、瀚高等；非关系型数据库：Hive、Hbase、MongoDB等。  3、攻击识别防御：支持对数据库SQL注入、缓冲区溢出等高危行为的识别防御。能够实时地监控所有到数据库的连接信息、操作数、违规数等。管理员可以断开指定的连接。  4、操作告警记录：对数据库高危操作、误操作等风险操作进行及时告警。对访问数据库的行为进行记录。  5、数据库审计策略：设备必须自带默认策略(如全审计、攻击特征)，支持自定义策略和规则，方便灵活配置审计规则。能支持不同数据库审计服务进行统一的策略制定、修改。  6、事件识别：支持以操作类型、时间、IP地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间等作为事件识别规则。  7、人工监测：通过网络安全服务专家人工监测分析的手段，对指定数据库执行5x8安全审计，对危险等级较高的威胁情报需在系统预警1小时内完成人工分析验证以甄别误报。  8、资源优化调整：按照公安部、公安厅考核要求及采购人管理需要，对杭州公安网络安全管理相关策略及配置进行修改或协调资源组织进行修改调整，确保与上级单位安全事件监测策略的一致性及安全事件监测的全面性。对设备及平台的底层日志与数据库日志进行分析，配合开发工程师对平台资源占用及运行稳定进行调整优化，确保各类网络安全设备及平台的正常运行。  二、投标人对系统提供服务：  1、定期巡检：协助采购人每季度至少一次对各类网络安全设备开展或督促组织巡检，对故障设备及软件平台开展运维响应，找到问题源头、联系厂商协调资源，实时排除各类故障、隐患。  2、资产梳理：配合采购人开展网络安全资产管理，实时掌握各类网络安全相关信息，确保各类网络安全管理制度落到实处。  3、技术支持：对采购人及各区县公安信息网安全管理平台中质量不合规的问题数据提供清理服务，每日查看并清理系统中的问题数据，对全市各区县、部门警种的安全管理技术问题提供远程技术支持，配合采购人为全市公安网络安全体系建设完善提供各类技术支持。  4、数据库审计服务能力须符合GB/T20945-2013《信息安全技术 信息系统安全审计产品技术要求和测评方法》（基本级）要求。 |
| 交付物 | 《数据库审计运维总结报告》  《网络安全巡检服务报告》（按季度提供） |
| **3、政务网云日志审计服务：**针对杭州市公安局的政务网提供日志审计服务。对网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，提供全维度、跨设备、细粒度的关联分析，提供真正可信赖的事件追责依据和业务运行的深度安全，确保业务的不间断运营安全。 | |
| 服务内容 | 因服务要求，政务网云日志审计服务需提供政务网云日志审计设备。提供不少于2套政务网日志审计（每套支持500个日志源授权）。 |
| 服务要求 | 1、管理设备授权可扩展：可提供授权扩展支持。  2、大数据联调功能：支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等功能。Kafka收发支持SSL加密。  3、日志代理：以Agent的方式提取日志并收集，能对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。  4、日志采集能力：可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。  5、日志解析能力：支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制免费扩展。支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息。  6、安全评估模型能力：评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。  7、应用性能监控：通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息（提供具备CMA资质或国家权威检测机构认可的第三方机构出具的检测报告）。  8、自定义资产拓扑：支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。  9、资产调研：配合采购人进行各个日志审计接入资产调研，统计资产数量，实时掌握接入资产的状态。  10、政务网云日志审计服务能力须符合GB/T 20945-2013 《信息安全技术信息系统安全审计产品安全技术要求和测试评价方法》（增强级）、《信息安全技术日志分析产品安全技术要求 GA/T 911-2010》(第三级)要求。 |
| 交付物 | 《日志审计运维总结报告》 |
| **4、政务网态势感知服务：**针对杭州市公安局的政务网业务系统，集成超大规模存查、大数据实时智能分析、行为分析、多维态势安全视图、安全联动闭环等安全模块。具备异构数据集成、核心数据安全分析、办公应用安全威胁挖掘等前沿大数据智能安全威胁挖掘分析与预警管控能力，提供全局态势感知和业务不间断稳定运行安全保障。 | |
| 服务内容 | 因服务要求，政务网态势感知服务需提供态势感知系统。提供1套政务网态势感知。 |
| 服务要求 | 1、支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序。  2、告警监控支持查看告警的基本信息、受害者、攻击者、处置响应、举证全文信息，其中受害者和攻击者支持查看响应ATT&CK矩阵视图，ATT&CK矩阵视图展示支持中文或英文的语言切换，布局支持侧面或下拉两种方式、并支持选择全部技术或子技术的展示等；处置响应支持处置响应闭环出来，可看到处置动作、告警调优、处置结果，及处置记录的全过程记录。  3、平台内置包括规则模型、关联模型、统计模型、情报模型、AI模型等安全分析模型，用户根据实际需求对上述模型进行添加、编辑、删除、复制等。  4、安全分析模型支持自定义新增，新添加的模型可选择适用的作用域，如全局通用、单选机构，如选择单选机构即选择应用的组织架构，可通过字段映射、静态值、模板、表达式等多种方式自定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容。  5、支持在告警详情中展示数据血缘关系，包括数据来源、原始日志、规则模型及原始告警，支持原始日志和规则模型的一键跳转，分别查看原始日志数据和相应的模型规则。  6、支持主机感染勒索病毒、网站被植入webshell、主机感染挖矿木马、主机感染恶意程序、主机被高危漏洞攻陷、主机被外部远控、内网横向攻击、内网横向探测、主机对外扫描、主机对外攻击、主机被爆破成功、发现APT攻击事件等10种以上的内置安全分析场景，针对分析场景支持至少3个任意字段聚合变量检索。  7、支持通过任务看板查看自动响应任务的数量、任务状态占比、任务趋势；以时间轴方式展示任务进行状态，并可查看每个阶段任务运行的详细信息。  8、平台具有统一的安全运营门户，作为重点关注功能的统一入口，如集成态势感知、Sherlock网络星空、通报预警、联动策略、运行监测等多个功能模块，实现平台功能的快速跳转；支持用户配置个人专属的统一门户，可配置项包括门户名称、菜单名称、应用图标等，且菜单内容支持自定义编辑，可链接平台以外的域名地址。 |
| 交付物 | 《政务网安全分析报告》（按季度提供） |
| **5、SaaS化安全服务：**针对杭州市公安局的政务网业务系统，提供SaaS化安全服务，快速发现业务系统的安全漏洞和安全隐患。SaaS化安全服务采用零部署云防护方案，具备DDoS清洗和云WAF功能；事后采用大数据分析形成可视化报告和统计分析报表；云监测服务实时准确的监测网站服务质量、安全事件、安全漏洞等多个维度的数据。 | |
| 服务内容 | 提供不超过10个主域名的云防护服务（每个主域名+10个子域名）；提供不超过10个主域名的云监测服务。 |
| 服务要求 | 一、云防护服务要求：  1、系统基于云化SaaS架构，无需消耗虚拟机资源或本地物理资源，通过云端服务平台完成站点管理，为用户提供云防护服务。  2、支持检查提交的报文是否符合HTTP协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等。  3、支持流量监测的功能，基于用户的访问记录，实时检查被访问页面的安全状况，能够发现更深层次的暗链、Webshell等安全事件。  4、日志采集能力：可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。  5、支持提供攻击防护安全策略，支持对命令注入（包括SQL注入、SQL盲注、代码注入等）、跨站脚本、SSI指令、路径穿越、远程文件包含、WebShell防护。  6、支持通过微信公众号查看网站整体防护态势，包含受攻击域名排行、攻击类型排行、攻击IP排行、攻击区域分布等状态信息。  7、具有云端7\*24远程安全专家服务能力，提供7\*24小时安全值守和应急响应服务。提供策略优化、配置调整、规则更新、问题处理、技术咨询安全事件通告等常规技术支持服务，实时监测感知持续性攻击、0day攻击等事件，并及时响应和对抗，同时在重大节会期间提供更高级别的安全响应服务。  二、云监测服务要求  1、全国范围内具备至少20个云监测服务节点。  2、支持大规模漏洞扫描服务能力，云端扫描引擎支持横向扩容，单个扫描任务扫描网站数量可达一万个以上。  3、支持按需提供周期性的网站安全云监测服务报告，报告应能对网站安全运行状况、漏洞情况、安全事件情况进行分析，并提供相应的修复建议以指导用户完成问题处置。  4、支持通过微信公众号实时了解用户名下站点的安全状态，展示漏洞威胁、安全事件和网站可用性相关监测数据。  5、支持通过短信、邮件方式向用户推送相关告警，告警类型包括网站服务质量不佳、安全事件告警、漏洞威胁告警。 |
| 交付物 | 《政务网业务系统安全分析报告》（按月度提供）  《网站安全云监测服务报告》 |
| **6、公安网安全风险感知服务：**用于强化杭州市公安局公安网安全风险感知能力。提供针对公安网的资产感知、安全基线、漏洞发现、弱口令检测、全流量威胁识别、大知攻击识别、主机安全监测与加固、白名单策略、主机层攻击链可视服务。通过网络流量镜像的方式进行采集并还原，提供流量资源进行分析。 | |
| 服务内容 | 提供不少于8次的安全风险感知服务支持 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、网络协议还原：对常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等。  2、文件协议还原:对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk等）、压缩格式文件（RAR、ZIP、GZ、7Z等）、文档类型文件（word、excel、pdf、rtf、ppt等）。  3、数据库协议还原：对常见数据库协议的识别或还原：DB2、Oracle、SQL Server、MySQL、PostgreSQL等协议。  4、会话流量还原：对TCP/UDP会话记录、异常流量会话记录、web访问记录、域名解析、SQL访问记录、邮件行为、登录情况、文件传输、FTP控制通道、SSL加密协商、telnet行为、IM通信等行为描述。  5、自定义协议还原：支持自定义协议和端口，满足特殊场景下的流量抓取。  6、攻击检测支持：支持暴力破解检测、Web攻击检测、网络攻击检测  7、攻击态势：提供全网攻击发现服务，并以态势大屏展现，包括整体网络风险指数、告警总数、攻击次数、攻击IP数、攻击源国家/地区TOP5、攻击态势，并支持自动翻转的攻击全景地图展示。  8、告警分析：对告警进行深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为。  9、威胁分析：对告警从威胁情报、应用安全、系统安全和设备安全的业务场景维度进行二次分析。应用安全的细分维度包括：WEB安全、数据库安全、邮件安全、中间件安全。系统安全的细分维度包括：主机爆破、弱口令、未授权行为、挖矿行为。  10、脆弱性分析：对全网脆弱性问题进行发现，为保证服务效果，服务厂商需拥有全国性的漏洞响应平台，累计发现10万个以上漏洞。  11、产品应以可视化方式提供指定时间段内：被监测网络中的特定主机与其他主机之间的相关联的已知、未知威胁事件与异常网络行为；被监测网络中指定威胁事件影响的主机以及相关联的其他威胁事件与异常网络行为；被监测网络中异常网络行为相关的主机和威胁事件；产品应可以采用智能化和自动化方式将多个相关联和类似的攻击时间进行归并。 |
| 交付物 | 《公安网安全风险感知服务分析报告》（按实际需求提供） |
| **7、公安网桌面云服务：**为保障杭州市公安局公安网访问过程安全可靠，有效防范数据泄露事件发生。通过桌面云技术提供公安日常办公，合作企业人员运维，需要实现分散部署、统一管理、提高运维效率，并通过数据不落地和多维度安全机制，保障访问过程安全可靠。通过超融合技术实现服务器的计算资源、存储资源、网络、安全的虚拟化，并通过容器技术承载本地公安业务系统和数据库，并提供业务网络主页微服务，实现业务系统的安全稳定。 | |
| 服务内容 | 因服务要求，公安网桌面云服务需提供瘦终端设备和桌面云授权。  1、提供不低于300点云桌面授权，不低于35台瘦终端。  2、平均每个人员使用的资源不低于2核8G内存和300G磁盘空间。 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、VDI授权类型：每用户授权支持发布个性化桌面、共享式桌面、虚拟应用3种资源类型。  2、公安办公软件兼容：可适配杭州市公安局公安日常办公软件，支持公安数据证书，流畅打开公安业务系统，并且可进行视频监控流畅的调阅。要求支持两种以上的Linux虚拟桌面操作系统，其中要包含国产Linux操作系统；为满足日后需求，要求适配银河麒麟操作系统。  3、自助快照恢复：当用户自己误操作导致云桌面卡慢、蓝屏、死机或者中病毒的时候，用户通过导航条按钮，可以自助进行系统盘快照还原操作。  4、云桌面连接可靠性：客户端连接虚拟桌面无需依赖虚拟机IP，在虚拟机网卡被禁用或被更改IP的情况下，云桌面业务不会中断，可防止因误操作而导致连接中断。  5、身份认证:多认证方式随需组合，包括账号密码、usb-key认证、短信认证、硬件特征绑定、动态口令等。  6、文件导出内容审计：开启文件安全导出后，虚拟机通过剪切板、PC设备和USB设备外发文件的操作将被禁止，用户可以使用虚拟机内部的文件导出工具实现文件外发，所有外发的文件内容都可以加密备份到数据中心，以备后续审计使用，可疑的导出行为会产生告警。  7、内置应用管控技术：管理组件实现全方位云桌面管控，可通过黑名单或白名单实现对禁止指定应用、进程的运行或只允许白名单内的应用、进程运行。  8、资产调研分配：配合采购人进行桌面云资产调研和分配，每周针对桌面云至少开展一次巡检服务，实时掌握桌面云使用情况。 |
| 交付物 | 《桌面云月度服务报告》（按月度提供） |
| **8、公安网一机两用服务：**针对杭州市公安局“一机两用”监控系统的稳定运行提供对应保障服务。提供对服务器漏洞扫描的准确性确认、对监控系统补丁下载率、防病毒软件覆盖率等数据的统计。 | |
| 服务内容 | 1、定期巡检服务，为杭州市公安局“一机两用”监控系统提供每月一次的巡检服务。  2、技术支持服务，每月10日至20日使用专用工具对服务器列表进行清理，确保每月服务器漏洞扫描工作的准确性；每月20日至下月10日，使用专用工具对杭州市公安局“一机两用”监控系统注册率、“一机两用”监控系统补丁下载率、防病毒软件覆盖率等公安部考核数据进行清理。 |
| 服务要求 | 产品升级服务:及时为采购人“一机两用”监控系统进行版本维护、升级，并为现场升级提供建议方案，协助做好产品的升级工作。 |
| 交付物 | 《一机两用巡检服务报告》（按月度提供）  《一机两用年度维保总结报告》  《考核技术支持服务报告》 |
| **9、视频网终端杀毒服务：**针对杭州市公安局视频专网终端进行病毒、木马、恶意软件等进查杀，提供主动防御、补丁管理功能。 | |
| 服务内容 | 因服务要求，视频网终端杀毒服务需提供PC终端和服务器授权。  提供不少于1500点PC终端和250点服务器授权。 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、国产化杀毒：针对中标麒麟/银河麒麟/普华/深度操作系统进行病毒查杀。  2、终端资产梳理统计：对终端PC信息进行收集，包括终端的硬件、软件、操作系统、网络、进程等信息。对接入视频网的PC终端进行统计，统计子网地址段地址使用率，显示地址段范围、大小、网关、已用数、可用数、已安装终端等信息。实时掌握终端杀毒软件的部署状态和运行情况。  3、病毒库更新：采用杀毒工具支持与浙江省公安厅杀毒软件级联，实时同步病毒库以及杀毒策略。  4、病毒查杀：要求通过多种杀毒引擎进行查杀，对恶意代码进行有效检测和识别，对已知、未知病毒、病毒变种提供全面检测、拦截和清除能力。提供至少两种杀毒引擎软件著作权。  5、终端立体防护：对PC终端提供立体防护服务，包含浏览器防护，系统防护，入口防护和隔离防护。  6、文件系统防护和访问控制：对所有文件或者程序及文档进行实时监控，提供对终端操作系统之间东西流量访问控制服务，包括基于数据包流向（任意/流入/流出）、协议（TCP/UDP/ICMP/TCP+UDP）、端口和IP的访问控制。  7、攻击拦截：能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质。支持U盘等移动磁盘设备和电脑硬盘间文件传输检测；支持局域网共享文件传输检测。  8、黑白名单扫描：支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件。  9、控制中心支持级联管理，可支持与浙江省公安厅视频专网终端防病毒控制中心级联。  10、对敲诈者病毒提供专有的防护功能。  11、支持按CVE编号查询漏洞，支持按KB号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务  12、简化补丁运维工作，支持补丁灰度发布，支持设置对特定分组优先进行补丁分发，自定义测试一段时间后再全网升级，实现补丁自动化运维。 |
| 交付物 | 《终端杀毒服务月度报告》（按月度提供） |
| **10、系统安全检测：**针对公安信息系统开展安全性测试和整体安全评估。模拟黑客使用的工具、分析方法对信息系统、网站等进行非破坏性质的攻击性测试，由工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题，发现存在的安全漏洞，输出测试报告，针对性提出加固建议，作为漏洞修复和加固整改的参考依据。 | |
| 服务内容 | 不少于6次系统安全检测。 |
| 服务要求 | 1、安全架构评估：首先对公安信息系统进行系统分析，分析其网络架构，软件体系以及程序部署等，然后再对新上线系统做系统安全分析，在这之后对系统进行安全建模，明确系统可能来自的各个潜在威胁，之后剖析系统，确认有哪些攻击界面，依次进行安全测试。  2、系统漏洞扫描：采用具有自主知识产权的漏洞扫描工具对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层面的扫描与分析，并对具体漏洞提出解决方案。  3、安全配置检查：根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具对信息系统中的主机系统、数据库与网络设备的脆弱性进行分析。  4、应用安全扫描：采用web应用漏洞扫描工具，通过定制的扫描规则，形成安全扫描策略文档，对指定网站进行自动化安全扫描，人工验证扫描结果输出安全扫描报告及修复建议。  5、渗透测试：模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，通过侵入系统，获取系统控制权并将入侵的过程和细节生成报告进行提交，由此检验系统所存在的安全威胁和风险，并能及时提醒安全管理员完善安全策略。 |
| 交付物 | 《系统安全检测总结报告》（按实际需求提供） |
| **11、网络安全检查：**在上级网络安全监管部门对杭州市局范围内开展网络安全检查、护网行动等工作前，配合采购人从安全技术、管理和运营等多个维度着手针对全市各警种、区县分局的公安业务系统开展安全检查、协助整改，完善网络安全保障措施。 | |
| 服务内容 | 不少于3次网络安全检查。 |
| 服务要求 | 1、在上级部门开展网络安全检查前，能够配合采购人先行开展安全检查，协助整改完成；  2、在上级部门开展检查期间提供技术支撑配合、值守保障等； |
| 交付物 | 《网络安全检查总结报告》（按实际需求提供） |
| **12、重保**：在重大活动时期，除驻点人员外，需另派遣不少于1名专业工程师驻场值守，对杭州市公安局重要系统进行安全保障。 | |
| 服务内容 | 不少于3次重大活动安全保障。 |
| 服务要求 | 针对杭州市公安局重要IT系统资产、包括主机、网络、应用等系统运行维护场景，在项目实施过程中，针对采购人信息安全建设需求，提供相关安全值守，值守工作内容包含但不限于以下内容：信息安全通告、信息安全咨询、对外服务检查、web站点渗透测试、安全漏洞扫描、主机安全检查、业务系统安全监测、安全值守、安全日志分析、应急响应等。针对重大活动安全保障，要求5分钟内电话响应。 |
| 交付物 | 《重大活动安全保障总结报告》（按实际需求提供） |
| **13、应急响应：**发生或可能发生安全事件时，投标人应快速响应并到达现场，协助进行安全事件处理，直到安全事件排除。 | |
| 服务内容 | 1、在服务期内，发生或可能发生安全事件时，投标人应快速响应并到达现场，协助进行安全事件处理，直到安全事件排除。对于影响业务的安全设备故障，在进行故障处理时，应先考虑业务恢复，然后再彻底解决故障。如投标人工程师不能在时限内解决问题，则应调动安全专家协助解决。  2、按需提供应急响应服务，不少于8次。 |
| 服务要求 | 1、紧急安全事件应急响应（网站被篡改或被攻击，网站被仿冒；某个业务全部瘫痪，重要数据丢失或被篡改，核心网络流量严重异常或瘫痪等）。接到电话通知后，必须15分钟内做出响应，1小时内到达现场。如1小时内无法解决问题，30分钟内调动安全专家协助解决。  2、严重安全事件应急响应（某个业务部分不可用，某个区域出现流量严重异常或瘫痪，安全设备硬件故障造成网络中断，网站访问速度严重变慢等）。接到电话通知后，必须15分钟内做出响应，2小时内到达现场。如2小时内无法解决问题，1小时内调动安全专家协助解决。  3、一般安全事件应急响应（业务使用存在异常，某个区域出现流量异常，发现安全漏洞隐患未进行修补的，病毒事件以及其他一般事件）。接到电话通知后，必须30分钟内做出响应，4小时内到达现场。如4小时内无法解决问题，2小时内调动安全专家协助解决。 |
| 交付物 | 《应急响应报告》（按实际需求提供） |
| **14、边界通道租赁服务：**数据交换前置服务器集群、双单向光闸池和数据交换后置服务器集群，组成3条边界通道，每条边界通道包括数据交换前置服务器、数据交换后置服务器。 | |
| 服务内容 | 因服务要求，边界通道租赁服务需提供通道。  共3条通道，每条都为（2+4+2）池化架构或其他架构来确保两侧交换系统及进出各单向2光闸的冗余能力，包含外侧防火墙。 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、服务性能：吞吐量≥8Gbps；数据库同步速率（1KB）≥12000条/秒；FTP文件同步速率（40KB）≥2600个/秒；消息同步速率（1KB）≥7000个/秒；传输时延≤50ms。  2、技术架构：支持集群化扩展，无需独立集群管理节点，具备集群节点并行交换、负载均衡和容灾切换功能（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  3、部署模式：交换前置和交换后置支持非对称部署。  4、数据库同步：支持异构数据库异构同步、多对一同步、一对多同步、全量同步、增量同步、定时任务同步、自定义主键同步方式等功能。  5、文件共享交换：支持FTP、SFTP、SMB、NFS，支持文件断点续传，支持大文件（GB级）同步。  6、文件同步：支持文件目录双向同步、镜像同步、源端删除同步、更新同步、累加同步、文件同步重名等同步策略。  7、API交换：支持前端API用户对后端Web资源访问、API反向代理；支持API调用方Token身份认证、数据格式检查、关键字过滤、请求报文完整性验证功能（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  8、API接口认证：Http Basic认证、Soap头认证、JWT认证、HMAC 签名认证等功能（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  9、敏感信息字段处理：加插数据水印，并支持通过数据水印溯源（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  10、敏感数据脱敏：数据库表中姓名、身份证号码、手机号码、详细地址等敏感或隐私信息的字段进行数据脱敏（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。 |
| 交付物 | 《边界通道服务总结报告》 |

**1、总体要求**

（1）本项目中服务涉及多张公安业务网络，不同服务内容对应不同技术要求，均应当满足各服务内容中对应的服务要求。

（2）系统安全检测服务中使用的工具软件必须为正版产品。

（3）网络安全检查过程中进行的渗透测试，在渗透测试之前必须要先提供相应的技术方案与采购人技术人员充分沟通,不能影响各项业务的正常进行，对一些可能引发事故的测试项要在采购人可控制的情况下以单独授权的方式进行。

（4）实施过程中应尽可能小的影响系统和网络的正常运行,做好备份和应急措施,不能对采购人应用系统的正常运行产生影响,包括系统性能明显下降、网络拥塞、服务中断等,如无法避免出现这些情况应先停止项目实施,并向采购人书面详细描述。

（5）服务期内提供7\*24小时的技术支持（包括电话咨询与现场服务）。在服务期内，发生或可能发生应急事件时，中标人应快速响应并到达现场，协助进行应急事件处理，直到应急事件排除。对于影响服务的故障，在进行故障处理时，应先考虑服务恢复，再彻底解决故障。如中标人工程师不能在时限内解决问题，则应调动专家协助解决。中标人在接到应急电话后，须在应急响应服务规定的时限内响应。

（6）中标人需协助采购人完成安全检查工作。

（7）中标人应在完成服务后五个工作日内提交相关报告，所有报告均以纸质版提交（需经采购人经办人、审核人、供应商签字并加盖公章）。

（8）中标人应针对本项目建立健全相应的管理制度，包括日常管理规章制度、内部岗位责任制度（包括各岗位职责等）、管理运作制度、考核制度（包括考核机制、激励机制、监督机制等）等。

（9）中标人应针对本项目建立紧急事件处理应急方案，包括建立运行服务保障应急预案、对可能遇到的问题具有相应的应对措施，在服务期间巡检、故障处理的组织和联系机制等。

**2、人员要求**

投标人须为本项目组织项目小组，保障各项服务内容的顺利开展。

投标人提供不少于2名驻点人员提供安全服务。

**2.1项目组人员要求**

（1）按照实际工作需求为本项目配备项目小组，并明确人员分工职责（须包含一名项目负责人）。

（2）人员服务时间：项目负责人、服务团队人员提供7\*24小时响应服务，接到采购人通知后，应在半小时内响应，如需提供现场服务，需在2小时内到达采购人指定地点。

（3）人员配备标准：除2名驻点人员外，项目组人员中须配备至少2名人员具有信息安全工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）或系统集成项目管理工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）。

（4）工作职责：项目负责人主要负责本次项目的实施以及采购人的对接工作。项目团队人员应有明确的岗位分配，各岗位有专人负责，需提供人员配置表，保障工作顺利有序进行。

**2.2驻点人员要求**

（1）提供2名全日制专科以上计算机专业学历，具有1年以上网络安全工作经验，年龄55周岁（含）以下，提供5\*8小时现场驻点服务（采购人提供办公工位）。至少1名需具备以下能力：

①熟练掌握各类安全技术，具有开展安全咨询和安全服务的经验；

②了解网络信息安全相关技能，如传统网络安全、网络攻防。

③具有编写网络规划方案能力熟悉网络安全解决方案能力。

④具备文档、汇报材料编写能力。

⑤熟练掌握主流安全设备的运行维护操作。

⑥信息安全工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）或系统集成项目管理工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）。

（2）驻点人员服务内容

1.负责安全监控、监测系统的日常运行状态巡查。

2.负责采购单位的资产梳理。

3.负责日常安全事件、安全威胁的响应处理。

4.负责定期对安全设备（系统）日志进行分析、处理，并提交报告。

5.提供新增服务器杀毒软件安装、策略优化、安全加固服务。

6.每月、季、年度编制并提交安全工作专题报告。

7.用户安排的其他网络与信息安全相关工作。

**2.3驻点人员变动**

投标人派出驻点人员必须达到采购人服务要求，经过采购人认可方可上岗（需提供资质证明材料、投标人和拟派人员共同出具保证能在本项目服务期间为本项目服务的承诺函）。

驻点人员应相对稳定，人员变动需提前1个月征求采购人意见并经采购人书面同意，投标人应在其人员变动后4小时响应，24小时内保证更换人员到位，且更换人员资历不低于投标时人员资历，并确保任何时候无人员缺位现象发生。

**3、保密要求**

①投标人应当对涉及采购人的信息严格保密，确保派遣的工作人员严格遵守保密纪律。投标人需和采购人签订保密协议，不得将信息泄露给第三方（包括但不限于合同期内）。否则，采购人有保留追究法律责任的权利。

②采购人应当对投标人及工作人员开展常态化安全保密教育，组织签订安全保密承诺书，明确具体安全管理内容、安全保密义务和责任。投标人应当严格按照采购人规定使用、存储、处理文档资料和数据。合同终止时，投标人应当交还全部资料和数据。

③投标人及工作人员违反安全管理要求，构成违法犯罪的，采购人应当及时报送本级政府采购和市场监督管理部门，提请列入政府采购严重违法失信行为记录名单、市场监督管理严重失信名单，并追究相关责任。

**4、投标人网络安全责任和义务：**

①明确投标人法定代表人为合作事项网络安全第一责任人，具体承担合作事项的部门主要负责人为直接责任人。

②不得转包合同任务。

③投标人应制订与合作事项相关的网络安全保障方案和网络安全事件应急预案。

④投标人发现网络安全漏洞、缺陷或者其他严重网络安全风险，应及时向采购人报告。

⑤处理合作事项的信息平台应当优先采用安全可信的硬件和软件产品。

⑥发生可能影响合作事项的网络安全重大事项，包括负责人及重要工作人员变更、业务转型、合并重组和投资并购等，投标人应提前向采购人报告。

⑦采用社会公共网络平台实施合作事项时，严禁涉及国家秘密和警务工作秘密。

⑧投标人应每年向采购人提交网络安全报告。

⑨其他应当落实的网络安全责任和义务。

**5、知识产权：**

投标人应保证用户在使用投标标的物或其任何一部分时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，那么投标人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；投标人已获取的知识产权归承建方所有，若涉及定制化部分的知识产权均归属于用户。

**（六）、商务要求**

1.服务期限：2024年6月1日至2025年5月31日。

2.实施地点：杭州市公安局。

3.付款方式：项目采用分期付款方式，具体如下

|  |  |  |
| --- | --- | --- |
| 序号 | 付款比例（%） | 付款方式 |
| 1 | 第一期付款:签订合同后5个工作日内，采购人向投标人支付合同总价40%。同时，收取合同总价1%的履约保证金。 | 国库转账支付 |
| 2 | 第二期付款：服务至2024年11月30日，经验收合格后,凭双方签字盖章的验收意见、验收小组签字的验收报告、月度考核表、验收资料等材料，经采购人对服务报告质量及数量审核无误后，根据合同单价、实际维护内容及数量按实结算，最多支付至250万元（含采购人已向投标人支付的第一期合同价款）； | 国库转账支付 |
| 3 | 第三期付款：至服务期结束，经验收合格后，凭双方签字盖章的验收意见、验收小组签字的验收报告、月度考核表、公示截图、验收资料等材料，经采购人对服务报告质量及数量审核无误后，根据合同单价、实际维护内容及数量按实结算剩余应付的合同款项，同时扣除投标人应向采购人支付的违约金。 | 国库转账支付 |
| 双方确认，采购人按前款结算并向投标人支付的款项总额不超过合同总价。  前述采购人按合同单价、实际维护内容及数量与投标人进行结算付款的方式不影响投标人承担其因未全面履行本项目义务而产生的相应违约金。 | | |

**（七）采购项目的其他要求**

**①验收：**

1、采购人按照《杭州市政府采购履约验收暂行办法》（杭财采监[2019]10号）规定组织对投标人履约的验收。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，投标人须承担由此发生的一切损失和费用，并接受相应的处理。

2、严格按照采购合同开展履约验收。采购人委托第三方机构组织验收，成立验收小组（验收小组由5人组成：其中采购人1名，专家4名（由采购代理机构从浙江政府采购网政府采购云政企区平台专家库中随机抽取），按照采购合同的约定对投标人履约情况进行验收，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，出具验收报告并经验收小组全体成员签字。采购人根据验收报告形成验收意见并经采购人与投标人签字盖章。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。

3、本项目为信息化运维项目，根据《杭州市公安局信息化项目管理办法》第27条规定,信息化运维项目服务期满后,项目单位应向市公安局科信局提交《信息化运维项目验收表》及验收所需相应材料,由市公安局科信局按照杭州市政府采购履约验收相关管理办法的程序,结合市局相关内控制度组织开展验收。

4、验收合格的项目，采购人将根据采购合同的约定及时向投标人支付采购资金、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》。

5、验收产生的费用首次验收费用由采购人承担，如首次验收不合格，后续验收费用由投标人支付。

6、验收内容及资料要求：

6.1验收内容

|  |  |  |
| --- | --- | --- |
| 序号 | 验收内容 | 验收标准 |
| 1 | 响应程度 | “等保测评服务”、“数据库审计服务”、“政务网云日志审计服务”、“政务网态势感知服务”、“SaaS化安全服务”、“公安网安全风险感知服务”、“公安网桌面云服务”、“公安网一机两用服务”、“视频网终端杀毒服务”、“系统安全检测”、“网络安全检查”、“重保”、“应急响应”、“边界通道租赁服务”十四部分维护内容的具体合同与招标文件要求响应程度。 |
| 2 | 人员情况 | 技术人员的数量、技术水平专业达到采购要求 |
| 3 | 响应时间情况 | 故障响应时间按照要求实施响应。 |
| 4 | 运维资料  报告提供情况 | 整体测评实施方案、等级保护测评报告、等级保护整改建议书、数据库审计运维总结报告、网络安全巡检服务报告、日志审计运维总结报告、政务网安全分析报告、政务网业务系统安全分析报告、网站安全云监测服务报告、公安网安全风险感知服务分析报告、桌面云月度服务报告、一机两用巡检服务报告、一机两用年度维保总结报告、考核技术支持服务报告、终端杀毒服务月度报告、系统安全检测总结报告、网络安全检查总结报告（如有）、重大活动安全保障总结报告、应急响应报告、边界通道服务总结报告等资料。 |
| 5 | 保密管理 | 投标人签订保密协议，遵守具体安全管理内容，履行安全保密义务和责任，未发生重大数据丢失和泄漏问题。 |
| 6 | 网络安全责任和义务 | 网络安全责任和义务达到合同要求。 |
| 7 | 中小、小微企业预留份额 | 中小、小微企业预留份额达到合同要求。 |
| 8 | 其他工作 | 履行项目采购文件、投标文件、合同条款中涉及的其他承诺的情况。 |

6.2验收资料清单如下：

验收资料要求包括（不限于）以下内容：

1. 采购文件
2. 投标文件
3. 采购合同
4. 考核表：（考核表由采购人经办人、审核人、投标人经办人签字盖章确认）。
5. 人员清单及其他材料：驻点人员及团队人员明细清单、驻点人员每月社保缴纳清单、驻点人员每日考勤签到记录、相关人员资历证明、相关人员资质证书、人员变更审批单（如有）、整体测评实施方案、等级保护测评报告、等级保护整改建议书、数据库审计运维总结报告、网络安全巡检服务报告、日志审计运维总结报告、政务网安全分析报告、政务网业务系统安全分析报告、网站安全云监测服务报告、公安网安全风险感知服务分析报告、桌面云月度服务报告、一机两用巡检服务报告、一机两用年度维保总结报告、考核技术支持服务报告、终端杀毒服务月度报告、系统安全检测总结报告、网络安全检查总结报告（如有）、重大活动安全保障总结报告、应急响应报告、边界通道服务总结报告；
6. 月、季、年度安全工作专题报告；
7. 日常保密教育资料、单位保密协议、个人保密承诺书；
8. 网络安全保障方案、网络安全事件应急预案、网络安全风险书面报告（如有）、网络安全重大事项书面报告（如有）；
9. 中小企业佐证材料、小微企业佐证材料；
10. 分包协议（如有）；

（11）其他需提供的相关材料。

**②考核：**

服务期内，采购人将对投标人进行月度考核，采取100分制计分方式，每扣1分扣违约金200元。如果投标人月度考核结果低于80分的，应递交书面整改报告。如投标人月度考核结果低于60分、或连续两个月度考核结果低于70分、或连续三个月度考核结果低于80分，采购人有权没收投标人全部履约保证金，并通知投标人解除合同，如给采购人造成损失的有权向投标人提出索赔。

如考核周期内重复出现相同扣分情形，累计计算扣除分值。

**月度考核表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **考核时间：** | |  | **填表日期：** | **年 月 日** |
| **投标人：** | |  | | |
| **序号** | **考核内容** | | **扣分情况** | **备注** |
| **（一）考核扣分项** | | |  |  |
| 1 | 针对等保测评服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 2 | 针对数据库审计服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 3 | 针对政务网云日志审计服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 4 | 针对政务网态势感知服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 5 | 针对SaaS化安全服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 6 | 针对公安网安全风险感知服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 7 | 针对公安网桌面云服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 8 | 针对公安网一机两用服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 9 | 针对视频网终端杀毒服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 10 | 针对系统安全检测服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 11 | 针对网络安全检查服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 12 | 针对重要时期重大活动安全保障服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 13 | 针对应急响应服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 14 | 针对边界通道租赁服务，投标人未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 15 | 投标人人员配备要求达不到合同条款要求的，每发生一次扣5分。 | |  |  |
| 16 | 投标人在服务期内未提供7\*24小时的技术支持（包括电话咨询与现场服务）。投标人在接到应急电话后，未在应规定时间内响应，每发生一次扣3分。 | |  |  |
| 17 | 投标人未协助采购人完成安全检查工作，每发生一次扣3分。 | |  |  |
| 18 | 投标人未按照要求提供文档，每发生一次扣5分。 | |  |  |
| 19 | 投标人发生违反相关保密规定、未按网络安全履行责任和义务的,每发生一次扣除违约金10000元/次外，采购人将追究投标人一切法律责任。 | |  |  |
| 20 | 未按承诺预留中小企业的比例达到合同总价的43%、小微企业的比例达到合同总价的28%，采购人有权无条件终止合同,并没收投标人全部履约保证金（如有），报送本级政府采购监管部门，提前列入失信行为记录名单，追究相关责任，且投标人应向采购人支付合同总价30%的违约金。 | |  |  |
| 项目经办人（签字）： 投标人项目负责人（签字盖章）：  项目审核人（签字盖章）： 日 期： | | | | |

**（八）采购标的对应的中小企业划分标准所属行业**

（1）按照《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300号）的所属行业规定，本项目采购标的：杭州市公安业务网安全服务项目，所属行业：(十二）软件和信息技术服务业。

**第四部分** **评标办法**

**评标办法前附表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评标标准 | 权重 | 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 | **根据投标人针对本项目的服务能力：**  **1、等保测评服务中所使用的安全测评工具软件：**（1）等保工具箱（2）商用密码检测工具（3）软件测试工具（4）代码审计工具。  **2、数据库审计服务：**（1）模块支持、（2）数据库类型支持、（3）攻击识别防御、（4）操作告警记录、（5）数据库审计策略、（6）事件识别、（7）人工监测、（8）资源优化调整。  **3、政务网云日志审计服务：**（1）大数据联调功能、（2）日志采集能力、（3）日志解析能力、（4）安全评估模型能力、（5）应用性能监控[提供具备CMA资质或国家权威检测机构认可的第三方机构出具的检测报告]。  **4、政务网态势感知服务：（**1）安全模块集成、（2）前沿大数据智能安全威胁挖掘分析与预警管控能力。  **5、SaaS化安全服务：**（1）流量监测功能、（2）日志采集能力、（3）攻击防护安全策略、（4）云监测服务节点、（5）大规模漏洞扫描服务能力。  **6、公安网安全风险感知服务：**（1）攻击态势、（2）告警分析、（3）威胁分析、（4）脆弱性分析  **7、公安网桌面云服务:**（1）身份认证系统需提供2个种认证方式组合的身份认证登录截图证明（2）文件导出内容审计(3)内置应用管控技术。  **8、视频网终端杀毒服务：**（1）病毒库更新、（2）病毒查杀、（3）终端立体防护、（4）文件系统防护和访问控制、（5）攻击拦截、（6）黑白名单扫描、（7）控制中心支持级联管理、（8）支持按CVE编号查询漏洞，支持按KB号查询漏洞，（9）简化补丁运维工作。  提供软件或系统功能截图，并明确需求中对应的服务要求，每项不满足扣1分，满分33分，扣完为止。截图材料不满足采购需求对应服务要求或无有效证明材料不得分,要求提供具备CMA资质或国家权威检测机构认可的第三方机构出具的检测报告的，必须提供检测报告，否则不得分。截图以投标人提供的盖章材料为依据。 | 33 | 客观分 | 一、服务能力 |
| 2 | 投标人提供（1）公安网桌面云服务桌面授权和瘦终端数量满足采购需求（2）视频网终端杀毒服务pc终端和服务器授权数量满足采购需求，满足采购文件要求每项得2分，不满足不得分，最高得分4分 | 4 | 客观分 |
| 3 | 投标人提供系统安全检测服务维护内容方案包括安全架构评估、系统漏洞扫描、安全配置检查、应用安全扫描、渗透测试，方案内容完整且合理、可行，符合采购需求的得2分，不满足的不得分。 | 2 | 主观分 |
| 4 | 投标人提供网络安全检查服务承诺   1. 在上级部门开展网络安全检查前，能够配合采购人先行开展安全检查，协助整改完成； 2. 在上级部门开展检查期间提供技术支撑配合、值守保障等；   承诺每项满足得1分，不满足不得分，最高得分2分。 | 2 | 客观分 |
| 5 | 投标人提供重要时期重大活动安全保障服务承诺在重大活动时期，除驻点人员外，另派遣不少于1名专业工程师驻场值守，对杭州市公安局重要系统进行安全保障，承诺满足得2分，不满足不得分。 | 2 | 客观分 |
| 6 | 投标人提供应急响应服务承诺  （1）紧急安全事件应急响应：接到电话通知后，必须15分钟内做出响应，1小时内到达现场。如1小时内无法解决问题，30分钟内调动安全专家协助解决。  （2）严重安全事件应急响应：接到电话通知后，必须15分钟内做出响应，2小时内到达现场。如2小时内无法解决问题，1小时内调动安全专家协助解决。  （3）一般安全事件应急响应；接到电话通知后，必须30分钟内做出响应，4小时内到达现场。如4小时内无法解决问题，2小时内调动安全专家协助解决。  承诺每项满足得1分，不满足不得分，最高得分3分。 | 3 | 客观分 |
| 7 | 投标人提供边界通道租赁服务维护满足：   1. 采用集群技术架构，支持集群化扩展，无需独立集群管理节点，具备集群节点并行交换、负载均衡和容灾切换功能； 2. 支持API交换，支持前端API用户对后端Web资源访问、API反向代理；支持API调用方Token身份认证、数据格式检查、关键字过滤、请求报文完整性验证功能。   （3）API接口认证：Http Basic认证、Soap头认证、JWT认证、HMAC 签名认证等功能。  （4）敏感信息字段处理：加插数据水印，并支持通过数据水印溯源。  （5）敏感数据脱敏：数据库表中姓名、身份证号码、手机号码、详细地址等敏感或隐私信息的字段进行数据脱敏。  每项满足得1分，不满足不得分，最高得分5分。  证明材料:提供具有CMA资质的第三方检测机构出具的检测报告或其他国家权威机构出具的检测报告并加盖公章。 | 5 | 客观分 |
| 8 | 投标人针对本项目建立健全相应的管理制度，包括(1)日常管理规章制度、(2)内部岗位责任制度（包括各岗位职责等）、(3)管理运作制度、(4)考核制度（包括考核机制、激励机制、监督机制等）等，服务方案每项满足需求得1分，不满足不得分，最高得分4分。  投标人针对本项目建立紧急事件处理应急方案，包括建立运行服务保障应急预案、对可能遇到的问题具有相应的应对措施，在服务期间巡检、故障处理的组织和联系机制等。服务方案满足需求得2分，不满足不得分。 | 6 | 主观分 | 二、总体服务方案 |
| 9 | 投标人提供项目小组：   1. 按照实际工作需求为本项目配备项目小组，并明确人员分工职责（须包含一名项目负责人）。 2. 人员服务时间：提供7\*24小时服务 3. 人员配备标准：除2名驻点人员外，项目组人员中须配备至少2名人员具有信息安全工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）或系统集成项目管理工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）。   每项满足得2分，不满足不得分，最高得分6分。 | 6 | 客观分 | 三、人员要求 |
| 1、投标人提供2名驻点人员：（1）全日制专科以上计算机专业学历；（2）具有1年以上网络安全工作经验；（3）年龄55周岁（含）以下；  2、其中的1名驻点人员：（1）人员能力符合采购需求要求。  每项满足得3分，不满足不得分，最高得分12分。 | 12 |
| 10 | 投标人承诺应在完成服务后五个工作日内提交相关报告，所有报告均以纸质版提交（需经采购人经办人、审核人、供应商签字并加盖公章）。承诺满足得1分，不满足不得分。 | 1 | 客观分 | 四、服务报告 |
| 11 | 承诺接受采购人对投标人及工作人员开展常态化安全保密教育，签订安全保密承诺书，遵守具体安全管理内容，履行安全保密义务和责任。承诺满足得2分，不满足不得分。 | 2 | 客观分 | 五、保密承诺 |
| 12 | 投标人类似项目建设的成功经验（2分）：至投标截止时间近三年以来投标人承担类似项目的情况，结合已完工的相关服务案例和用户反应情况，参考合同复印件及用户验收报告等实例证明（以合同签订时间为准），每个合同得1分，最高得2分。（原件备查，采购人在项目评审直至合同签订、履约期间，有权要求投标人出具投标文件中的主要业绩证明原件：如合同及用户验收报告等，予以确认其的真实性和有效性，如出现与事实不符等情况，将根据有关规定以“提供虚假材料谋取中标”予以处罚）。 | 2 | 客观分 | 六、业绩 |
| 13 | 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）\*20］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。  落实政府采购政策需要进行价格调整的，以调整后的价格计算评标基准价和投标报价。 | 20 | 客观分 | / |

\***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。推进采购需求和评审因素编制的科学化和精细化，评审小组成员个人主观打分偏离所有评审小组成员主观打分平均值30%以上的，由评审委员会启动评分畸高、畸低行为认定程序，限制专家自由裁量权。

**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;

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 投标文件不满足招标文件的其它实质性要求的；

4.2.14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，采购代理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、采购代理机构沟通并作书面记录。采购人、采购代理机构确认后，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**

**（服务类）**

**第一部分 合同书**

项目名称： 杭州市公安业务网安全服务项目

甲方：

乙方：

签订地：

签订日期： 年 月 日

年月日，杭州市公安局以（公开招标方式）对杭州市公安业务网安全服务项目进行了采购。经 评标委员会 评定，（中标供应商名称）为该项目中标供应商。现于中标通知书发出之日起十个工作日内，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、诚实信用和绿色的原则，经（甲方）(以下简称：甲方)和 （中标供应商名称） (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：杭州市公安业务网安全服务项目，主要工作内容为保证杭州市公安局公安业务网和数据的安全稳定运行，通过采购等保测评服务、数据库审计服务、政务网云日志审计服务、政务网态势感知服务、SaaS化安全服务、公安网安全风险感知服务、公安网桌面云服务、公安网一机两用服务、视频网终端杀毒服务、系统安全检测、网络安全检查、重保、应急响应、边界通道租赁服务，提升杭州市公安局公安业务网网络与数据安全的能力。

1.2.2 服务标准：根据采购文件确定的技术指标或者服务要求确定验收指标和标准。未进行相应约定的，应当符合国家强制性规定、政策要求、安全标准、行业或企业有关标准等。

**1.3 价款**

本项目采用以下第1.3.2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）。

1.3.2单价合同。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合同金额￥元（大写：元人民币）。合同价格清单：详见附件1，人员清单：详见附件2。

1.3.3其他计价方式： / 。**1.4履约保证金**

1.4.1履约保证金的比例为合同金额的 1 %；

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且收到乙方退还履约保证金申请之日起 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**

1.5.1预付款比例、支付方式、时间详见 ***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***；

**1.8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。

**2.0 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”系指甲方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，甲方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甲方履行的除货物和工程以外的其他政府采购对象，包括甲方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甲方；甲方委托采购代理机构代表其与乙方签订合同的，甲方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**

2.10.1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 等保测评服务、边界通道租赁服务、公安网一机两用服务、公安网桌面云服务 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。

2.10.2乙方采取分包方式履行合同的，甲方可直接向分包供应商支付款项。

2.10.3分包内容详见附件5。

**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。

1.3.2服务工作量的计量方式为：根据合同单价、实际维护内容及数量按实结算。

**1.4.2**本项目要求乙方提交履约保证金，乙方应按约定的方式，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，提交不超过合同金额1%的履约保证金；鼓励和支持乙方以银行、保险公司出具的保函形式提供履约保证，乙方以银行、保险公司出具保函形式提交履约保证金的，甲方不得拒收。

**1.5.1**预付款比例、支付方式、时间

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，甲方在5个工作日内予以支付。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。

甲方在政府采购合同中约定预付款，预付款金额为合同价款的40%；乙方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。

乙方可以登录：<http://czj.hangzhou.gov.cn/zfcg（杭州市政府采购网），在线发起付款申请和提交发票，并可以在线查询支付信息。具体操作指南可以查询该网站文件《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）。>

**1.6.2**资金支付的方式、时间和条件：

|  |  |  |
| --- | --- | --- |
| 序号 | 付款比例（%） | 付款方式 |
| 1 | 第一期付款:签订合同后5个工作日内，甲方向乙方支付合同总价40%。同时，收取合同总价1%的履约保证金。 | 国库转账支付 |
| 2 | 第二期付款：服务至2024年11月30日，经验收合格后,凭双方签字盖章的验收意见、验收小组签字的验收报告、月度考核表、验收资料等材料，经甲方对服务报告质量及数量审核无误后，根据合同单价、实际维护内容及数量按实结算，最多支付至250万元（含甲方已向乙方支付的第一期合同价款）； | 国库转账支付 |
| 3 | 第三期付款：至服务期结束，经验收合格后，凭双方签字盖章的验收意见、验收小组签字的验收报告、月度考核表、公示截图、验收资料等材料，经甲方对服务报告质量及数量审核无误后，根据合同单价、实际维护内容及数量按实结算剩余应付的合同款项，同时扣除乙方应向甲方支付的违约金。 | 国库转账支付 |
| 双方确认，甲方按前款结算并向乙方支付的款项总额不超过合同总价。  前述甲方按合同单价、实际维护内容及数量与乙方进行结算付款的方式不影响乙方承担其因未全面履行本项目义务而产生的相应违约金。 | | |

**1.7.1** 服务交付（实施）的时间（期限）：12个月，2024年6月1日至2025年5月31日。

**1.7.2** 服务交付（实施）的地点（地域范围）：杭州市公安局。

**1.8.7**违约责任：

（1）乙方应完全按照甲方招标文件的要求和乙方投标文件及相关文件承诺完成本项目，因乙方自身财务、技术、人力等原因导致项目风险的，应承担全部责任。

（2）甲方有权依据有关法律法规、政府管理的相关职能规定，对本项目进行监督和检查，有权要求乙方按照监督检查情况制定相应措施并加以整改。甲方不因行使该监督和检查权而承担任何责任，也不因此减轻或免除乙方根据合同约定或相关法律法规规定应承担的任何义务或责任。

（3）拟签订的合同文本要求乙方提交履约保证金的，乙方应当以支票、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。履约保证金的数额为采购合同金额的1%，在项目通过验收且甲方收到乙方退还履约保证金申请之日起5个工作日内凭双方签字盖章的验收意见无息退还。

（4）乙方每延迟一日缴纳履约保证金，违约金则按应缴纳的履约保证金金额的0.05%计算，最高限额为本合同履约保证金的20%；乙方逾期10日，未按要求缴纳履约保证金的，甲方有权单方面解除合同，并就由此造成的一切损失均由乙方负责赔偿。服务期满，通过验收，甲方于收到乙方退还履约保证金申请之日起5个工作日内凭双方签字盖章的验收意见，无息退还乙方履约保证金。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%。

（5）除不可抗力外，如果乙方没有按照本合同约定的期限、地点和方式提供服务，那么甲方可要求乙方支付违约金，违约金按每迟延提供服务一日的应提供而未提供服务价格的2.5%计算，最高限额为本合同总价的20%；迟延提供服务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，并有权对乙方追究一切责任。

（6）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。

（7）乙方擅自将本合同的全部或部分事务转由第三人（经甲方书面同意的分包人除外）承担，甲方可解除本合同，且乙方应按合同总价的30％向甲方支付违约金。如发生损失的，乙方还应赔偿甲方损失。

（8）服务期间，甲方每月对乙方实施考核，如有违约的，根据考核条款进行处置，直至解除合同。

（9）本项目履约过程中，乙方未按承诺预留中小企业的比例达到合同总价的43%、小微企业的比例达到合同总价的28%，甲方有权无条件终止合同,并没收乙方全部履约保证金（如有），报送本级政府采购监管部门，提前列入失信行为记录名单，追究相关责任，且乙方应向甲方支付合同总价30%的违约金。

（10）乙方发生违反相关保密规定、未按网络安全履行责任和义务的,每发生一次扣除违约金10000元/次外，甲方将追究乙方一切法律责任。

（11）因乙方或乙方人员工作过错造成的安全管理事故，乙方负全部责任及相关费用。

（12）乙方所有人员的事故由乙方自行全权负责。

（13）违约金在结算合同尾款时一次性扣除。

**1.9**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1.9.2条款规定的方式解决：

**1.9.1**将争议提交杭州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**向甲方所在地的人民法院起诉。

**2.3.2**具有知识产权的计算机软件等货物的知识产权归属：本项目为服务项目，若服务中涉及计算机软件等货物的知识产权归属乙方所有，甲方享有服务期内和服务相关的使用权。

**2.5** 结算方式和付款条件详见第1.6.2条款规定

**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***15个工作日***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***7个工作日***内以书面形式通知对方当事人，并在***10个工作日***内，将有关部门出具的证明文件送达对方当事人。

**2.15.1**履约验收时间：本项目分期验收，第一期初验验收：服务期至2023年11月30日，第二期终验验收：服务期结束后。

**2.15.3**

1、甲方按照《杭州市政府采购履约验收暂行办法》（杭财采监[2019]10号）规定组织对乙方履约的验收。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，乙方须承担由此发生的一切损失和费用，并接受相应的处理。

2、严格按照采购合同开展履约验收。甲方委托第三方机构组织验收，成立验收小组（验收小组由5人组成：其中甲方1名，专家4名由采购代理机构从浙江政府采购网政府采购云政企区平台专家库中随机抽取产生），按照采购合同的约定对乙方履约情况进行验收，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，出具验收报告并经验收小组全体成员签字。甲方根据验收报告形成验收意见并经甲方与乙方签字盖章。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。

3、本项目为信息化运维项目，根据《杭州市公安局信息化项目管理办法》第27条规定,信息化运维项目服务期满后,项目单位应向市公安局科信局提交《信息化运维项目验收表》及验收所需相应材料,由市公安局科信局按照杭州市政府采购履约验收相关管理办法的程序,结合市局相关内控制度组织开展验收。

4、验收合格的项目，甲方将根据采购合同的约定及时向乙方支付采购资金、退还履约保证金。验收不合格的项目，甲方将依法及时处理。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》。

5、验收产生的费用首次验收费用由甲方承担，如首次验收不合格，后续验收费用由乙方支付。

6、验收内容及资料要求：

6.1验收内容

|  |  |  |
| --- | --- | --- |
| 序号 | 验收内容 | 验收标准 |
| 1 | 响应程度 | “等保测评服务”、“数据库审计服务”、“政务网云日志审计服务”、“政务网态势感知服务”、“SaaS化安全服务”、“公安网安全风险感知服务”、“公安网桌面云服务”、“公安网一机两用服务”、“视频网终端杀毒服务”、“系统安全检测”、“网络安全检查”、“重保”、“应急响应”、“边界通道租赁服务”十四部分维护内容的具体合同与招标文件要求响应程度。 |
| 2 | 人员情况 | 技术人员的数量、技术水平专业达到采购要求 |
| 3 | 响应时间情况 | 故障响应时间按照要求实施响应。 |
| 4 | 运维资料  报告提供情况 | 整体测评实施方案、等级保护测评报告、等级保护整改建议书、数据库审计运维总结报告、网络安全巡检服务报告、日志审计运维总结报告、政务网安全分析报告、政务网业务系统安全分析报告、公安网安全风险感知服务分析报告、桌面云月度服务报告、一机两用巡检服务报告、一机两用年度维保总结报告、终端杀毒服务月度报告、系统安全检测总结报告、网络安全检查总结报告（如有）、重大活动安全保障总结报告、应急响应报告、边界通道服务总结报告等资料。 |
| 5 | 保密管理 | 乙方签订保密协议，遵守具体安全管理内容，履行安全保密义务和责任，未发生重大数据丢失和泄漏问题。 |
| 6 | 网络安全责任和义务 | 网络安全责任和义务达到合同要求。 |
| 7 | 中小、小微企业预留份额 | 中小、小微企业预留份额达到合同要求。 |
| 8 | 其他工作 | 履行项目采购文件、投标文件、合同条款中涉及的其他承诺的情况。 |

6.2验收资料清单如下：

验收资料要求包括（不限于）以下内容：

1. 采购文件
2. 投标文件
3. 采购合同
4. 考核表：（考核表由甲方经办人、审核人、乙方经办人签字盖章确认）。
5. 人员清单及其他材料：驻点人员及团队人员明细清单、驻点人员每月社保缴纳清单、驻点人员每日考勤签到记录、相关人员资历证明、相关人员资质证书、人员变更审批单（如有）、整体测评实施方案、等级保护测评报告、等级保护整改建议书、数据库审计运维总结报告、网络安全巡检服务报告、日志审计运维总结报告、政务网安全分析报告、政务网业务系统安全分析报告、网站安全云监测服务报告、公安网安全风险感知服务分析报告、桌面云月度服务报告、一机两用巡检服务报告、一机两用年度维保总结报告、考核技术支持服务报告、终端杀毒服务月度报告、系统安全检测总结报告、网络安全检查总结报告（如有）、重大活动安全保障总结报告、应急响应报告、边界通道服务总结报告；
6. 月、季、年度安全工作专题报告；
7. 日常保密教育资料、单位保密协议、个人保密承诺书；
8. 网络安全保障方案、网络安全事件应急预案、网络安全风险书面报告（如有）、网络安全重大事项书面报告（如有）；
9. 中小企业佐证材料、小微企业佐证材料；
10. 分包协议（如有）；

（11）其他需提供的相关材料。

**2.19**本合同壹式陆份，具有同等法律效力，甲乙双方各执叁份。

**3、服务内容**

|  |  |
| --- | --- |
| 1、等保测评服务：针对甲方的重要信息系统提供等保测评服务。 | |
| 服务内容 | 1、对于测评结论符合等保要求的，出具测评报告及整改建议书。  2、对于测评结论不符合等保要求的，出具差距分析报告及整改建议书。  3、本项目服务期内测评系统数量不少于25个。 |
| 服务要求 | 1、测评依据：须根据国家标准GB/T 22239-2019：《信息安全技术网络安全等级保护基本要求》要求选取安全基础指标开展检测工作，并出具符合国家相关规范要求的测评报告。  2、实施方案：乙方对具体测评系统详细了解的基础上，编制针对性的等级保护测评整体实施方案，包括项目概述、等保测评范围和内容、项目实施流程、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。  3、运行环境：安全测评需要的运行环境（如场地、网络环境等）由甲方提供，乙方应详细描述需要的运行环境的具体要求。  4、项目实施流程：乙方应具有等保工具箱、商用密码检测工具、软件测试工具、代码审计工具。本次等级保护测评实施过程中所使用到的工具软件由乙方推荐，需经甲方确认后方由乙方提供并在测评中使用。乙方应在投标文件中详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。 |
| 交付物 | 《信息系统安全等级保护备案表》（初次测评系统）  《信息系统安全等级保护定级报告》（初次测评系统）  《整体测评实施方案》  《等级保护测评报告》  《等级保护整改建议书》 |
| **2、数据库审计服务：**针对杭州市公安局的政务外网、视频专网和公安网提供数据库审计服务，满足等级保护的合规性需求，同时配合相关人工服务对数据库审计内容进行处理，发现存在的问题及时研判、预警、处理，建立完备安全保障机制。对杭州公安各类安全违规事件进行实时监测、实时预警，协助甲方及时、有效开展整改，切实降低各类安全风险，有效减少部、省、市上级网络安全管理职能部门的各类安全事件通报。配合相关人工服务进行日常运维。 | |
| 服务内容 | 因服务要求，数据库审计服务需提供数据库审计设备。政务网不少于2套（不限制支持的数据库实例个数）、视频专网不少于4台、公安网不少于6台。 |
| 服务要求 | 一、该服务需要提供以下的服务要求支持：  1、模块支持：数据库审计、风险漏洞扫描、状态监控、敏感数据扫描等功能。  2、数据库类型支持：国际主流数据库： Oracle、MySQL、SQLserver、DB2、Sybase、Informix、Teradata、PostgreSQL、Access、cache等；国产数据库：达梦、南大通用、人大金仓、神通、瀚高等；非关系型数据库：Hive、Hbase、MongoDB等。  3、攻击识别防御：支持对数据库SQL注入、缓冲区溢出等高危行为的识别防御。能够实时地监控所有到数据库的连接信息、操作数、违规数等。管理员可以断开指定的连接。  4、操作告警记录：对数据库高危操作、误操作等风险操作进行及时告警。对访问数据库的行为进行记录。  5、数据库审计策略：设备必须自带默认策略(如全审计、攻击特征)，支持自定义策略和规则，方便灵活配置审计规则。能支持不同数据库审计服务进行统一的策略制定、修改。  6、事件识别：支持以操作类型、时间、IP地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间等作为事件识别规则。  7、人工监测：通过网络安全服务专家人工监测分析的手段，对指定数据库执行5x8安全审计，对危险等级较高的威胁情报需在系统预警1小时内完成人工分析验证以甄别误报。  8、资源优化调整：按照公安部、公安厅考核要求及甲方管理需要，对杭州公安网络安全管理相关策略及配置进行修改或协调资源组织进行修改调整，确保与上级单位安全事件监测策略的一致性及安全事件监测的全面性。对设备及平台的底层日志与数据库日志进行分析，配合开发工程师对平台资源占用及运行稳定进行调整优化，确保各类网络安全设备及平台的正常运行。  二、乙方对系统提供服务：  1、定期巡检：协助甲方每季度至少一次对各类网络安全设备开展或督促组织巡检，对故障设备及软件平台开展运维响应，找到问题源头、联系厂商协调资源，实时排除各类故障、隐患。  2、资产梳理：配合甲方开展网络安全资产管理，实时掌握各类网络安全相关信息，确保各类网络安全管理制度落到实处。  3、技术支持：对甲方及各区县公安信息网安全管理平台中质量不合规的问题数据提供清理服务，每日查看并清理系统中的问题数据，对全市各区县、部门警种的安全管理技术问题提供远程技术支持，配合甲方为全市公安网络安全体系建设完善提供各类技术支持。  4、数据库审计服务能力须符合GB/T20945-2013《信息安全技术 信息系统安全审计产品技术要求和测评方法》（基本级）要求。 |
| 交付物 | 《数据库审计运维总结报告》  《网络安全巡检服务报告》（按季度提供） |
| **3、政务网云日志审计服务：**针对杭州市公安局的政务网提供日志审计服务。对网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，提供全维度、跨设备、细粒度的关联分析，提供真正可信赖的事件追责依据和业务运行的深度安全，确保业务的不间断运营安全。 | |
| 服务内容 | 因服务要求，政务网云日志审计服务需提供政务网云日志审计设备。提供不少于2套政务网日志审计（每套支持500个日志源授权）。 |
| 服务要求 | 1、管理设备授权可扩展：可提供授权扩展支持。  2、大数据联调功能：支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等功能。Kafka收发支持SSL加密。  3、日志代理：以Agent的方式提取日志并收集，能对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。  4、日志采集能力：可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。  5、日志解析能力：支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制免费扩展。支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息。  6、安全评估模型能力：评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。  7、应用性能监控：通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  8、自定义资产拓扑：支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息。  9、资产调研：配合甲方进行各个日志审计接入资产调研，统计资产数量，实时掌握接入资产的状态。  10、政务网云日志审计服务能力须符合GB/T 20945-2013 《信息安全技术信息系统安全审计产品安全技术要求和测试评价方法》（增强级）、《信息安全技术日志分析产品安全技术要求 GA/T 911-2010》(第三级)要求。 |
| 交付物 | 《日志审计运维总结报告》 |
| **4、政务网态势感知服务：**针对杭州市公安局的政务网业务系统，集成超大规模存查、大数据实时智能分析、行为分析、多维态势安全视图、安全联动闭环等安全模块。具备异构数据集成、核心数据安全分析、办公应用安全威胁挖掘等前沿大数据智能安全威胁挖掘分析与预警管控能力，提供全局态势感知和业务不间断稳定运行安全保障。 | |
| 服务内容 | 因服务要求，政务网态势感知服务需提供态势感知系统。提供1套政务网态势感知。 |
| 服务要求 | 1、支持安全态势的可视化呈现，以大屏的方式从攻击事件、资产安全、追踪溯源、运行监测、重保方案等多个维度进行可视化展示，并可根据“组织架构”筛选大屏展示数据范围，支持自定义大屏轮播时间和大屏轮播顺序。  2、告警监控支持查看告警的基本信息、受害者、攻击者、处置响应、举证全文信息，其中受害者和攻击者支持查看响应ATT&CK矩阵视图，ATT&CK矩阵视图展示支持中文或英文的语言切换，布局支持侧面或下拉两种方式、并支持选择全部技术或子技术的展示等；处置响应支持处置响应闭环出来，可看到处置动作、告警调优、处置结果，及处置记录的全过程记录。  3、平台内置包括规则模型、关联模型、统计模型、情报模型、AI模型等安全分析模型，用户根据实际需求对上述模型进行添加、编辑、删除、复制等。  4、安全分析模型支持自定义新增，新添加的模型可选择适用的作用域，如全局通用、单选机构，如选择单选机构即选择应用的组织架构，可通过字段映射、静态值、模板、表达式等多种方式自定义分析模型的告警名称、威胁等级、告警类型、攻击链、可选字段、告警描述、处置建议等内容。  5、支持在告警详情中展示数据血缘关系，包括数据来源、原始日志、规则模型及原始告警，支持原始日志和规则模型的一键跳转，分别查看原始日志数据和相应的模型规则。  6、支持主机感染勒索病毒、网站被植入webshell、主机感染挖矿木马、主机感染恶意程序、主机被高危漏洞攻陷、主机被外部远控、内网横向攻击、内网横向探测、主机对外扫描、主机对外攻击、主机被爆破成功、发现APT攻击事件等10种以上的内置安全分析场景，针对分析场景支持至少3个任意字段聚合变量检索。  7、支持通过任务看板查看自动响应任务的数量、任务状态占比、任务趋势；以时间轴方式展示任务进行状态，并可查看每个阶段任务运行的详细信息。  8、平台具有统一的安全运营门户，作为重点关注功能的统一入口，如集成态势感知、Sherlock网络星空、通报预警、联动策略、运行监测等多个功能模块，实现平台功能的快速跳转；支持用户配置个人专属的统一门户，可配置项包括门户名称、菜单名称、应用图标等，且菜单内容支持自定义编辑，可链接平台以外的域名地址。 |
| 交付物 | 《政务网安全分析报告》（按季度提供） |
| **5、SaaS化安全服务：**针对杭州市公安局的政务网业务系统，提供SaaS化安全服务，快速发现业务系统的安全漏洞和安全隐患。SaaS化安全服务采用零部署云防护方案，具备DDoS清洗和云WAF功能；事后采用大数据分析形成可视化报告和统计分析报表；云监测服务实时准确的监测网站服务质量、安全事件、安全漏洞等多个维度的数据。 | |
| 服务内容 | 提供不超过10个主域名的云防护服务（每个主域名+10个子域名）；提供不超过10个主域名的云监测服务。 |
| 服务要求 | 一、云防护服务要求：  1、系统基于云化SaaS架构，无需消耗虚拟机资源或本地物理资源，通过云端服务平台完成站点管理，为用户提供云防护服务。  2、支持检查提交的报文是否符合HTTP协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等。  3、支持流量监测的功能，基于用户的访问记录，实时检查被访问页面的安全状况，能够发现更深层次的暗链、Webshell等安全事件。  4、日志采集能力：可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。  5、支持提供攻击防护安全策略，支持对命令注入（包括SQL注入、SQL盲注、代码注入等）、跨站脚本、SSI指令、路径穿越、远程文件包含、WebShell防护。  6、支持通过微信公众号查看网站整体防护态势，包含受攻击域名排行、攻击类型排行、攻击IP排行、攻击区域分布等状态信息。  7、具有云端7\*24远程安全专家服务能力，提供7\*24小时安全值守和应急响应服务。提供策略优化、配置调整、规则更新、问题处理、技术咨询安全事件通告等常规技术支持服务，实时监测感知持续性攻击、0day攻击等事件，并及时响应和对抗，同时在重大节会期间提供更高级别的安全响应服务。  二、云监测服务要求  1、全国范围内具备至少20个云监测服务节点。  2、支持大规模漏洞扫描服务能力，云端扫描引擎支持横向扩容，单个扫描任务扫描网站数量可达一万个以上。  3、支持按需提供周期性的网站安全云监测服务报告，报告应能对网站安全运行状况、漏洞情况、安全事件情况进行分析，并提供相应的修复建议以指导用户完成问题处置。  4、支持通过微信公众号实时了解用户名下站点的安全状态，展示漏洞威胁、安全事件和网站可用性相关监测数据。  5、支持通过短信、邮件方式向用户推送相关告警，告警类型包括网站服务质量不佳、安全事件告警、漏洞威胁告警。 |
| 交付物 | 《政务网业务系统安全分析报告》（按月度提供）  《网站安全云监测服务报告》 |
| **6、公安网安全风险感知服务：**用于强化杭州市公安局公安网安全风险感知能力。提供针对公安网的资产感知、安全基线、漏洞发现、弱口令检测、全流量威胁识别、大知攻击识别、主机安全监测与加固、白名单策略、主机层攻击链可视服务。通过网络流量镜像的方式进行采集并还原，提供流量资源进行分析。 | |
| 服务内容 | 提供不少于8次的安全风险感知服务支持 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、网络协议还原：对常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等。  2、文件协议还原:对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk等）、压缩格式文件（RAR、ZIP、GZ、7Z等）、文档类型文件（word、excel、pdf、rtf、ppt等）。  3、数据库协议还原：对常见数据库协议的识别或还原：DB2、Oracle、SQL Server、MySQL、PostgreSQL等协议。  4、会话流量还原：对TCP/UDP会话记录、异常流量会话记录、web访问记录、域名解析、SQL访问记录、邮件行为、登录情况、文件传输、FTP控制通道、SSL加密协商、telnet行为、IM通信等行为描述。  5、自定义协议还原：支持自定义协议和端口，满足特殊场景下的流量抓取。  6、攻击检测支持：支持暴力破解检测、Web攻击检测、网络攻击检测  7、攻击态势：提供全网攻击发现服务，并以态势大屏展现，包括整体网络风险指数、告警总数、攻击次数、攻击IP数、攻击源国家/地区TOP5、攻击态势，并支持自动翻转的攻击全景地图展示。  8、告警分析：对告警进行深度行为分析，行为包括DNS解析行为、TCP/UDP交互行为、WEB访问行为、传输文件行为。  9、威胁分析：对告警从威胁情报、应用安全、系统安全和设备安全的业务场景维度进行二次分析。应用安全的细分维度包括：WEB安全、数据库安全、邮件安全、中间件安全。系统安全的细分维度包括：主机爆破、弱口令、未授权行为、挖矿行为。  10、脆弱性分析：对全网脆弱性问题进行发现，为保证服务效果，服务厂商需拥有全国性的漏洞响应平台，累计发现10万个以上漏洞。  11、产品应以可视化方式提供指定时间段内：被监测网络中的特定主机与其他主机之间的相关联的已知、未知威胁事件与异常网络行为；被监测网络中指定威胁事件影响的主机以及相关联的其他威胁事件与异常网络行为；被监测网络中异常网络行为相关的主机和威胁事件；产品应可以采用智能化和自动化方式将多个相关联和类似的攻击时间进行归并。 |
| 交付物 | 《公安网安全风险感知服务分析报告》（按实际需求提供） |
| **7、公安网桌面云服务：**为保障杭州市公安局公安网访问过程安全可靠，有效防范数据泄露事件发生。通过桌面云技术提供公安日常办公，合作企业人员运维，需要实现分散部署、统一管理、提高运维效率，并通过数据不落地和多维度安全机制，保障访问过程安全可靠。通过超融合技术实现服务器的计算资源、存储资源、网络、安全的虚拟化，并通过容器技术承载本地公安业务系统和数据库，并提供业务网络主页微服务，实现业务系统的安全稳定。 | |
| 服务内容 | 因服务要求，公安网桌面云服务需提供瘦终端设备和桌面云授权。  1、提供不低于300点云桌面授权，不低于35台瘦终端。  2、平均每个人员使用的资源不低于2核8G内存和300G磁盘空间。 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、VDI授权类型：每用户授权支持发布个性化桌面、共享式桌面、虚拟应用3种资源类型。  2、公安办公软件兼容：可适配杭州市公安局公安日常办公软件，支持公安数据证书，流畅打开公安业务系统，并且可进行视频监控流畅的调阅。为保障国产化办公需要，要求支持两种以上的Linux虚拟桌面操作系统，其中要包含国产Linux操作系统；为满足日后国产化需求，要求提供银河麒麟的兼容性认证报告。  3、自助快照恢复：当用户自己误操作导致云桌面卡慢、蓝屏、死机或者中病毒的时候，用户通过导航条按钮，可以自助进行系统盘快照还原操作。  4、云桌面连接可靠性：客户端连接虚拟桌面无需依赖虚拟机IP，在虚拟机网卡被禁用或被更改IP的情况下，云桌面业务不会中断，可防止因误操作而导致连接中断。  5、身份认证:多认证方式随需组合，包括账号密码、usb-key认证、短信认证、硬件特征绑定、动态口令等。  6、文件导出内容审计：开启文件安全导出后，虚拟机通过剪切板、PC设备和USB设备外发文件的操作将被禁止，用户可以使用虚拟机内部的文件导出工具实现文件外发，所有外发的文件内容都可以加密备份到数据中心，以备后续审计使用，可疑的导出行为会产生告警。  7、内置应用管控技术：管理组件实现全方位云桌面管控，可通过黑名单或白名单实现对禁止指定应用、进程的运行或只允许白名单内的应用、进程运行。  8、资产调研分配：配合甲方进行桌面云资产调研和分配，每周针对桌面云至少开展一次巡检服务，实时掌握桌面云使用情况。 |
| 交付物 | 《桌面云月度服务报告》（按月度提供） |
| **8、公安网一机两用服务：**针对杭州市公安局“一机两用”监控系统的稳定运行提供对应保障服务。提供对服务器漏洞扫描的准确性确认、对监控系统补丁下载率、防病毒软件覆盖率等数据的统计。 | |
| 服务内容 | 1、定期巡检服务，为杭州市公安局“一机两用”监控系统提供每月一次的巡检服务。  2、技术支持服务，每月10日至20日使用专用工具对服务器列表进行清理，确保每月服务器漏洞扫描工作的准确性；每月20日至下月10日，使用专用工具对杭州市公安局“一机两用”监控系统注册率、“一机两用”监控系统补丁下载率、防病毒软件覆盖率等公安部考核数据进行清理。 |
| 服务要求 | 产品升级服务:及时为甲方“一机两用”监控系统进行版本维护、升级，并为现场升级提供建议方案，协助做好产品的升级工作。 |
| 交付物 | 《一机两用巡检服务报告》（按月度提供）  《一机两用年度维保总结报告》  《考核技术支持服务报告》 |
| **9、视频网终端杀毒服务：**针对杭州市公安局视频专网终端进行病毒、木马、恶意软件等进查杀，提供主动防御、补丁管理功能。 | |
| 服务内容 | 因服务要求，视频网终端杀毒服务需提供PC终端和服务器授权。  提供不少于1500点PC终端和250点服务器授权。 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、国产化杀毒：针对中标麒麟/银河麒麟/普华/深度操作系统进行病毒查杀。  2、终端资产梳理统计：对终端PC信息进行收集，包括终端的硬件、软件、操作系统、网络、进程等信息。对接入视频网的PC终端进行统计，统计子网地址段地址使用率，显示地址段范围、大小、网关、已用数、可用数、已安装终端等信息。实时掌握终端杀毒软件的部署状态和运行情况。  3、病毒库更新：采用杀毒工具支持与浙江省公安厅杀毒软件级联，实时同步病毒库以及杀毒策略。  4、病毒查杀：要求通过多种杀毒引擎进行查杀，对恶意代码进行有效检测和识别，对已知、未知病毒、病毒变种提供全面检测、拦截和清除能力。提供至少两种杀毒引擎软件著作权。  5、终端立体防护：对PC终端提供立体防护服务，包含浏览器防护，系统防护，入口防护和隔离防护。  6、文件系统防护和访问控制：对所有文件或者程序及文档进行实时监控，提供对终端操作系统之间东西流量访问控制服务，包括基于数据包流向（任意/流入/流出）、协议（TCP/UDP/ICMP/TCP+UDP）、端口和IP的访问控制。  7、攻击拦截：能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质。支持U盘等移动磁盘设备和电脑硬盘间文件传输检测；支持局域网共享文件传输检测。  8、黑白名单扫描：支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件。  9、控制中心支持级联管理，可支持与浙江省公安厅视频专网终端防病毒控制中心级联。  10、对敲诈者病毒提供专有的防护功能。  11、支持按CVE编号查询漏洞，支持按KB号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务  12、简化补丁运维工作，支持补丁灰度发布，支持设置对特定分组优先进行补丁分发，自定义测试一段时间后再全网升级，实现补丁自动化运维。 |
| 交付物 | 《终端杀毒服务月度报告》（按月度提供） |
| **10、系统安全检测：**针对公安信息系统开展安全性测试和整体安全评估。模拟黑客使用的工具、分析方法对信息系统、网站等进行非破坏性质的攻击性测试，由工程师进行深入的手工测试和分析，识别工具弱点扫描无法发现的问题，发现存在的安全漏洞，输出测试报告，针对性提出加固建议，作为漏洞修复和加固整改的参考依据。 | |
| 服务内容 | 不少于6次系统安全检测。 |
| 服务要求 | 1、安全架构评估：首先对公安信息系统进行系统分析，分析其网络架构，软件体系以及程序部署等，然后再对新上线系统做系统安全分析，在这之后对系统进行安全建模，明确系统可能来自的各个潜在威胁，之后剖析系统，确认有哪些攻击界面，依次进行安全测试。  2、系统漏洞扫描：采用具有自主知识产权的漏洞扫描工具对服务范围内各种软硬件设备进行网络层、系统层、数据库、应用层面的扫描与分析，并对具体漏洞提出解决方案。  3、安全配置检查：根据既定的检查规范及方法，采用人工检查用表（checklist）、脚本程序或基线扫描工具对信息系统中的主机系统、数据库与网络设备的脆弱性进行分析。  4、应用安全扫描：采用web应用漏洞扫描工具，通过定制的扫描规则，形成安全扫描策略文档，对指定网站进行自动化安全扫描，人工验证扫描结果输出安全扫描报告及修复建议。  5、渗透测试：模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，通过侵入系统，获取系统控制权并将入侵的过程和细节生成报告进行提交，由此检验系统所存在的安全威胁和风险，并能及时提醒安全管理员完善安全策略。 |
| 交付物 | 《系统安全检测总结报告》（按实际需求提供） |
| **11、网络安全检查：**在上级网络安全监管部门对杭州市局范围内开展网络安全检查、护网行动等工作前，配合甲方从安全技术、管理和运营等多个维度着手针对全市各警种、区县分局的公安业务系统开展安全检查、协助整改，完善网络安全保障措施。 | |
| 服务内容 | 不少于3次网络安全检查。 |
| 服务要求 | 1、在上级部门开展网络安全检查前，能够配合甲方先行开展安全检查，协助整改完成；  2、在上级部门开展检查期间提供技术支撑配合、值守保障等； |
| 交付物 | 《网络安全检查总结报告》（按实际需求提供） |
| **12、重保**：在重大活动时期，除驻点人员外，需另派遣不少于1名专业工程师驻场值守，对杭州市公安局重要系统进行安全保障。 | |
| 服务内容 | 不少于3次重大活动安全保障。 |
| 服务要求 | 针对杭州市公安局重要IT系统资产、包括主机、网络、应用等系统运行维护场景，在项目实施过程中，针对甲方信息安全建设需求，提供相关安全值守，值守工作内容包含但不限于以下内容：信息安全通告、信息安全咨询、对外服务检查、web站点渗透测试、安全漏洞扫描、主机安全检查、业务系统安全监测、安全值守、安全日志分析、应急响应等。针对重大活动安全保障，要求5分钟内电话响应。 |
| 交付物 | 《重大活动安全保障总结报告》（按实际需求提供） |
| **13、应急响应：**发生或可能发生安全事件时，乙方应快速响应并到达现场，协助进行安全事件处理，直到安全事件排除。 | |
| 服务内容 | 1、在服务期内，发生或可能发生安全事件时，乙方应快速响应并到达现场，协助进行安全事件处理，直到安全事件排除。对于影响业务的安全设备故障，在进行故障处理时，应先考虑业务恢复，然后再彻底解决故障。如乙方工程师不能在时限内解决问题，则应调动安全专家协助解决。  2、按需提供应急响应服务，不少于8次。 |
| 服务要求 | 1、紧急安全事件应急响应（网站被篡改或被攻击，网站被仿冒；某个业务全部瘫痪，重要数据丢失或被篡改，核心网络流量严重异常或瘫痪等）。接到电话通知后，必须15分钟内做出响应，1小时内到达现场。如1小时内无法解决问题，30分钟内调动安全专家协助解决。  2、严重安全事件应急响应（某个业务部分不可用，某个区域出现流量严重异常或瘫痪，安全设备硬件故障造成网络中断，网站访问速度严重变慢等）。接到电话通知后，必须15分钟内做出响应，2小时内到达现场。如2小时内无法解决问题，1小时内调动安全专家协助解决。  3、一般安全事件应急响应（业务使用存在异常，某个区域出现流量异常，发现安全漏洞隐患未进行修补的，病毒事件以及其他一般事件）。接到电话通知后，必须30分钟内做出响应，4小时内到达现场。如4小时内无法解决问题，2小时内调动安全专家协助解决。 |
| 交付物 | 《应急响应报告》（按实际需求提供） |
| **14、边界通道租赁服务：**数据交换前置服务器集群、双单向光闸池和数据交换后置服务器集群，组成3条边界通道，每条边界通道包括数据交换前置服务器、数据交换后置服务器。 | |
| 服务内容 | 因服务要求，边界通道租赁服务需提供通道。  共3条通道，每条都为（2+4+2）池化架构或其他架构来确保两侧交换系统及进出各单向2光闸的冗余能力，包含外侧防火墙。 |
| 服务要求 | 该服务需要提供以下的服务要求支持：  1、服务性能：吞吐量≥8Gbps；数据库同步速率（1KB）≥12000条/秒；FTP文件同步速率（40KB）≥2600个/秒；消息同步速率（1KB）≥7000个/秒；传输时延≤50ms。  2、技术架构：支持集群化扩展，无需独立集群管理节点，具备集群节点并行交换、负载均衡和容灾切换功能（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  3、部署模式：交换前置和交换后置支持非对称部署。  4、数据库同步：支持异构数据库异构同步、多对一同步、一对多同步、全量同步、增量同步、定时任务同步、自定义主键同步方式等功能。  5、文件共享交换：支持FTP、SFTP、SMB、NFS，支持文件断点续传，支持大文件（GB级）同步。  6、文件同步：支持文件目录双向同步、镜像同步、源端删除同步、更新同步、累加同步、文件同步重名等同步策略。  7、API交换：支持前端API用户对后端Web资源访问、API反向代理；支持API调用方Token身份认证、数据格式检查、关键字过滤、请求报文完整性验证功能（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  8、API接口认证：Http Basic认证、Soap头认证、JWT认证、HMAC 签名认证等功能（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  9、敏感信息字段处理：加插数据水印，并支持通过数据水印溯源（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。  10、敏感数据脱敏：数据库表中姓名、身份证号码、手机号码、详细地址等敏感或隐私信息的字段进行数据脱敏（提供具备CMA资质或国家权威机构认可的第三方机构出具的检测报告）。 |
| 交付物 | 《边界通道服务总结报告》 |

**4、总体要求**

（1）本项目中服务涉及多张公安业务网络，不同服务内容对应不同技术要求，均应当满足各服务内容中对应的服务要求。

（2）系统安全检测服务中使用的工具软件必须为正版产品。

（3）网络安全检查过程中进行的渗透测试，在渗透测试之前必须要先提供相应的技术方案与甲方技术人员充分沟通,不能影响各项业务的正常进行，对一些可能引发事故的测试项要在甲方可控制的情况下以单独授权的方式进行。

（4）实施过程中应尽可能小的影响系统和网络的正常运行,做好备份和应急措施,不能对甲方应用系统的正常运行产生影响,包括系统性能明显下降、网络拥塞、服务中断等,如无法避免出现这些情况应先停止项目实施,并向甲方书面详细描述。

（5）服务期内提供7\*24小时的技术支持（包括电话咨询与现场服务）。在服务期内，发生或可能发生应急事件时，乙方应快速响应并到达现场，协助进行应急事件处理，直到应急事件排除。对于影响服务的故障，在进行故障处理时，应先考虑服务恢复，再彻底解决故障。如乙方工程师不能在时限内解决问题，则应调动专家协助解决。乙方在接到应急电话后，须在应急响应服务规定的时限内响应。

（6）乙方需协助甲方完成安全检查工作。

（7）乙方应在完成服务后五个工作日内提交相关报告，所有报告均以纸质版提交（需经甲方经办人、审核人、乙方签字并加盖公章）。

（8）乙方应针对本项目建立健全相应的管理制度，包括日常管理规章制度、内部岗位责任制度（包括各岗位职责等）、管理运作制度、考核制度（包括考核机制、激励机制、监督机制等）等。

（9）乙方应针对本项目建立紧急事件处理应急方案，包括建立运行服务保障应急预案、对可能遇到的问题具有相应的应对措施，在服务期间巡检、故障处理的组织和联系机制等。

**5、人员要求**

乙方须为本项目组织项目小组，保障各项服务内容的顺利开展。

乙方提供不少于2名驻点人员提供安全服务。

**5.1项目组人员要求**

（1）按照实际工作需求为本项目配备项目小组，并明确人员分工职责（须包含一名项目负责人）。

（2）人员服务时间：项目负责人、服务团队人员提供7\*24小时响应服务，接到甲方通知后，应在半小时内响应，如需提供现场服务，需在2小时内到达甲方指定地点。

（3）人员配备标准：除2名驻点人员外，项目组人员中须配备至少2名人员具有信息安全工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）或系统集成项目管理工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）。

（4）工作职责：项目负责人主要负责本次项目的实施以及甲方的对接工作。项目团队人员应有明确的岗位分配，各岗位有专人负责，需提供人员配置表，保障工作顺利有序进行。

**5.2驻点人员要求**

（1）提供2名全日制专科以上计算机专业学历，具有1年以上网络安全工作经验，年龄55周岁（含）以下，提供5\*8小时现场驻点服务（甲方提供办公工位）。至少1名需具备以下能力：

①熟练掌握各类安全技术，具有开展安全咨询和安全服务的经验；

②了解网络信息安全相关技能，如传统网络安全、网络攻防。

③具有编写网络规划方案能力熟悉网络安全解决方案能力。

④具备文档、汇报材料编写能力。

⑤熟练掌握主流安全设备的运行维护操作。

⑥信息安全工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）或系统集成项目管理工程师（国家人力资源和社会保障部、工业和信息化部共同颁发）。

（2）驻点人员服务内容

1.负责安全监控、监测系统的日常运行状态巡查。

2.负责采购单位的资产梳理。

3.负责日常安全事件、安全威胁的响应处理。

4.负责定期对安全设备（系统）日志进行分析、处理，并提交报告。

5.提供新增服务器杀毒软件安装、策略优化、安全加固服务。

6.每月、季、年度编制并提交安全工作专题报告。

7.用户安排的其他网络与信息安全相关工作。

**5.3驻点人员变动**

乙方派出驻点人员必须达到甲方服务要求，经过甲方认可方可上岗（需提供资质证明材料、乙方和拟派人员共同出具保证能在本项目服务期间为本项目服务的承诺函）。

驻点人员应相对稳定，人员变动需提前1个月征求甲方意见并经甲方书面同意，乙方应在其人员变动后4小时响应，24小时内保证更换人员到位，且更换人员资历不低于投标时人员资历，并确保任何时候无人员缺位现象发生。

**6、保密要求**

①乙方应当对涉及甲方的信息严格保密，确保派遣的工作人员严格遵守保密纪律。乙方需和甲方签订保密协议，不得将信息泄露给第三方（包括但不限于合同期内）。否则，甲方有保留追究法律责任的权利。

②甲方应当对乙方及工作人员开展常态化安全保密教育，组织签订安全保密承诺书，明确具体安全管理内容、安全保密义务和责任。乙方应当严格按照甲方规定使用、存储、处理文档资料和数据。合同终止时，乙方应当交还全部资料和数据。

③乙方及工作人员违反安全管理要求，构成违法犯罪的，甲方应当及时报送本级政府采购和市场监督管理部门，提请列入政府采购严重违法失信行为记录名单、市场监督管理严重失信名单，并追究相关责任。

**7、乙方网络安全责任和义务：**

①明确乙方法定代表人为合作事项网络安全第一责任人，具体承担合作事项的部门主要负责人为直接责任人。

②不得转包合同任务。

③乙方应制订与合作事项相关的网络安全保障方案和网络安全事件应急预案。

④乙方发现网络安全漏洞、缺陷或者其他严重网络安全风险，应及时向甲方报告。

⑤处理合作事项的信息平台应当优先采用安全可信的硬件和软件产品。

⑥发生可能影响合作事项的网络安全重大事项，包括负责人及重要工作人员变更、业务转型、合并重组和投资并购等，乙方应提前向甲方报告。

⑦采用社会公共网络平台实施合作事项时，严禁涉及国家秘密和警务工作秘密。

⑧乙方应每年向甲方提交网络安全报告。

⑨其他应当落实的网络安全责任和义务。

**8、知识产权：**

乙方应保证用户在使用投标标的物或其任何一部分时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；乙方已获取的知识产权归承建方所有，若涉及定制化部分的知识产权均归属于用户。

**附件1：合同价格清单**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 内容 | 数量 | 单位 | 单价（元） | 总价（元） | 备注（中小、小微企业提供的服务内容） |
| 1 | 等保测评服务 | 1、对于测评结论符合等保要求的，出具测评报告及整改建议书。  2、对于测评结论不符合等保要求的，出具差距分析报告及整改建议书。  3、本项目服务期内测评系统数量不少于25个。 | 25 | 个 |  |  |  |
| 2 | 数据库审计服务 | 政务网不少于2套（不限制支持的数据库实例个数） | 2 | 套 |  |  |  |
| 视频专网不少于4台 | 4 | 台 |  |  |  |
| 公安网不少于6台 | 6 | 台 |  |  |  |
| 3 | 政务网云日志审计服务 | 提供不少于2套政务网日志审计（每  套支持500个日志源授权） | 2 | 套 |  |  |  |
| 4 | 政务网态势感知服务 | 提供1套政务网态势感知 | 1 | 套 |  |  |  |
| 5 | SaaS化安全服务 | 提供不超过10个主域名的云防护服务（每个主域名+10个子域名） | 10 | 个 |  |  |  |
| 提供不超过10个主域名的云监测服务 | 10 | 个 |  |  |  |
| 6 | 公安网安全风险感知服务 | 提供不少于8次的安全风险感知服务支持 | 8 | 次 |  |  |  |
| 7 | 公安网桌面云服务 | 提供不低于300点云桌面授权  （平均每个人员使用的资源不低于2核8G内存和300G磁盘空间） | 300 | 点 |  |  |  |
| 提供不低于35台瘦终端  （每台终端不低于2核8G内存和300G磁盘空间） | 35 | 台 |  |  |  |
| 8 | 公安网一机两用服务 | 1、定期巡检服务，为杭州市公安局“一机两用”监控系统提供每月一次的巡检服务。  2、技术支持服务，每月10日至20日使用专用工具对服务器列表进行清理，确保每月服务器漏洞扫描工作的准确性；每月20日至下月10日，使用专用工具对杭州市公安局“一机两用”监控系统注册率、“一机两用”监控系统补丁下载率、防病毒软件覆盖率等公安部考核数据进行清理。 | 1 | 项 |  |  |  |
| 9 | 视频网终端杀毒服务 | 提供不少于1500点PC终端 | 1500 | 点 |  |  |  |
| 提供不少于250点服务器授权 | 250 | 点 |  |  |  |
| 10 | 系统安全检测 | 不少于6次系统安全检测。 | 6 | 次 |  |  |  |
| 11 | 网络安全检查 | 不少于3次网络安全检查。 | 3 | 次 |  |  |  |
| 12 | 重保 | 不少于3次重大活动安全保障。 | 3 | 次 |  |  |  |
| 13 | 应急响应 | 按需提供应急响应服务，不少于8次。 | 8 | 次 |  |  |  |
| 14 | 边界通道租赁服务 | 共3条通道，每条都为（2+4+2）池化架构或其他架构来确保两侧交换系统及进出各单向2光闸的冗余能力，包含外侧防火墙。 | 3 | 条 |  |  |  |
| 合同总价人民币（小写） | |  | | | | | |
| 合同总价人民币（大写） | |  | | | | | |
| 其中：中小企业金额达到 元，占合同总价的 % | | | | | | | |
| 小微企业金额达到 元，占合同总价的 % | | | | | | | |

**附件2：项目人员清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 姓名 | 联系方式 | 身份证号码 | 人员资质证书 | 本项目承担的岗位 | 驻点情况 |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |

**附件3：考核**

服务期内，甲方将对乙方进行月度考核，采取100分制计分方式，每扣1分扣违约金200元。如果乙方月度考核结果低于80分的，应递交书面整改报告。如乙方月度考核结果低于60分、或连续两个月度考核结果低于70分、或连续三个月度考核结果低于80分，甲方有权没收乙方全部履约保证金，并通知乙方解除合同，如给甲方造成损失的有权向乙方提出索赔。

如考核周期内重复出现相同扣分情形，累计计算扣除分值。

**月度考核表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **考核时间：** | |  | **填表日期：** | **年 月 日** |
| **乙方：** | |  | | |
| **序号** | **考核内容** | | **扣分情况** | **备注** |
| **（一）考核扣分项** | | |  |  |
| 1 | 针对等保测评服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 2 | 针对数据库审计服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 3 | 针对政务网云日志审计服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 4 | 针对政务网态势感知服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 5 | 针对SaaS化安全服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 6 | 针对公安网安全风险感知服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 7 | 针对公安网桌面云服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 8 | 针对公安网一机两用服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 9 | 针对视频网终端杀毒服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 10 | 针对系统安全检测服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 11 | 针对网络安全检查服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 12 | 针对重要时期重大活动安全保障服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 13 | 针对应急响应服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 14 | 针对边界通道租赁服务，乙方未按采购需求要求提供服务，每发生一次扣3分。 | |  |  |
| 15 | 乙方人员配备要求达不到合同条款要求的，每发生一次扣5分。 | |  |  |
| 16 | 乙方在服务期内未提供7\*24小时的技术支持（包括电话咨询与现场服务）。乙方在接到应急电话后，未在应规定时间内响应，每发生一次扣3分。 | |  |  |
| 17 | 乙方未协助甲方完成安全检查工作，每发生一次扣3分。 | |  |  |
| 18 | 乙方未按照要求提供文档，每发生一次扣5分。 | |  |  |
| 19 | 乙方发生违反相关保密规定、未按网络安全履行责任和义务的,每发生一次扣除违约金10000元/次外，甲方将追究乙方一切法律责任。 | |  |  |
| 20 | 未按承诺预留中小企业的比例达到合同总价的43%、小微企业的比例达到合同总价的28%，甲方有权无条件终止合同,并没收乙方全部履约保证金（如有），报送本级政府采购监管部门，提前列入失信行为记录名单，追究相关责任，且乙方应向甲方支付合同总价30%的违约金。 | |  |  |
| 甲方项目经办人（签字）： 乙方项目负责人（签字盖章）：  项目审核人（签字盖章）： 日 期： | | | | |

**附件4：检测工具清单**

**附件5：分包协议（如有）**

**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**

杭州市公安局、浙江正浩招标代理有限公司：

我方参与杭州市公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】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

**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**

（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**

（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**

杭州市公安局、浙江正浩招标代理有限公司：

我方参加你方组织的杭州市公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】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）

2.3.2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）**

杭州市公安局、浙江正浩招标代理有限公司：

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公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】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）**

杭州市公安局、浙江正浩招标代理有限公司：

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公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】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

**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**

杭州市公安局、浙江正浩招标代理有限公司：

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）

杭州市公安局、浙江正浩招标代理有限公司：

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）的价格完成杭州市公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】的实施。

**开标一览表（报价表）(单位均为人民币元)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 内容 | 数量 | 单位 | 单价（元） | 总价（元） | 备注（中小、小微企业提供的服务内容） |
| 1 | 等保测评服务 | 1、对于测评结论符合等保要求的，出具测评报告及整改建议书。  2、对于测评结论不符合等保要求的，出具差距分析报告及整改建议书。  3、本项目服务期内测评系统数量不少于25个。 | 25 | 个 |  |  |  |
| 2 | 数据库审计服务 | 政务网不少于2套（不限制支持的数据库实例个数） | 2 | 套 |  |  |  |
| 视频专网不少于4台 | 4 | 台 |  |  |  |
| 公安网不少于6台 | 6 | 台 |  |  |  |
| 3 | 政务网云日志审计服务 | 提供不少于2套政务网日志审计（每  套支持500个日志源授权） | 2 | 套 |  |  |  |
| 4 | 政务网态势感知服务 | 提供1套政务网态势感知 | 1 | 套 |  |  |  |
| 5 | SaaS化安全服务 | 提供不超过10个主域名的云防护服务（每个主域名+10个子域名） | 10 | 个 |  |  |  |
| 提供不超过10个主域名的云监测服务 | 10 | 个 |  |  |  |
| 6 | 公安网安全风险感知服务 | 提供不少于8次的安全风险感知服务支持 | 8 | 次 |  |  |  |
| 7 | 公安网桌面云服务 | 提供不低于300点云桌面授权  （平均每个人员使用的资源不低于2核8G内存和300G磁盘空间） | 300 | 点 |  |  |  |
| 提供不低于35台瘦终端  （每台终端不低于2核8G内存和300G磁盘空间） | 35 | 台 |  |  |  |
| 8 | 公安网一机两用服务 | 1、定期巡检服务，为杭州市公安局“一机两用”监控系统提供每月一次的巡检服务。  2、技术支持服务，每月10日至20日使用专用工具对服务器列表进行清理，确保每月服务器漏洞扫描工作的准确性；每月20日至下月10日，使用专用工具对杭州市公安局“一机两用”监控系统注册率、“一机两用”监控系统补丁下载率、防病毒软件覆盖率等公安部考核数据进行清理。 | 1 | 项 |  |  |  |
| 9 | 视频网终端杀毒服务 | 提供不少于1500点PC终端 | 1500 | 点 |  |  |  |
| 提供不少于250点服务器授权 | 250 | 点 |  |  |  |
| 10 | 系统安全检测 | 不少于6次系统安全检测。 | 6 | 次 |  |  |  |
| 11 | 网络安全检查 | 不少于3次网络安全检查。 | 3 | 次 |  |  |  |
| 12 | 重保 | 不少于3次重大活动安全保障。 | 3 | 次 |  |  |  |
| 13 | 应急响应 | 按需提供应急响应服务，不少于8次。 | 8 | 次 |  |  |  |
| 14 | 边界通道租赁服务 | 共3条通道，每条都为（2+4+2）池化架构或其他架构来确保两侧交换系统及进出各单向2光闸的冗余能力，包含外侧防火墙。 | 3 | 条 |  |  |  |
| 投标总价人民币（小写） | |  | | | | | |
| 投标总价人民币（大写） | |  | | | | | |
| 其中：中小企业金额达到 元，占投标报价的 % | | | | | | | |
| 小微企业金额达到 元，占投标报价的 % | | | | | | | |

**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：采购代理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。）

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\_(采购人)\_单位的\_杭州市公安业务网安全服务项目\_\_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**

杭州市公安局、浙江正浩招标代理有限公司：

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公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】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公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】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、采购代理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 %，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、采购代理机构后，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）若成为杭州市公安业务网安全服务项目【招标编号：ZHZB-2024HZGA-02】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 %，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 杭州市公安局 的 杭州市公安业务网安全服务项目 采购活动，工程的施工单位全部为符合政策要求的中小企业（或者：服务全部由符合政策要求的中小企业承接）。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

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

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

……

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

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

投标人名称（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。