**2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务**

招标文件

**（电子招投标）**

编号: **HZSGAJ-2024-17（代)**

采购人：**杭州市公安局交通警察支队**

采购代理机构：**浙江信达咨询监理有限公司**

二〇二四年八月

**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

2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务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8月23日09点30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：HZSGAJ-2024-17（代)**

**项目名称：**2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务

**预算金额（元）：**8674500（其中2024年安排3469800元）

**最高限价（元）：**8544500

**采购需求：**2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务主要内容：本项目以购买服务方式，提供交通管理数据全生命周期运营服务、安全加固及应用迁移改造服务、货运导航数据及运营保障服务、安全防控风险预警服务，要求提供不少于11人驻点服务。

实施目标：通过本项目实施，提供常态化交通数据运维服务，为采购人正常业务运行提供数据支撑、模型支撑、技术保障支撑，完成采购人数据及应用安全迁移改造，实现数据及应用安全合规。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：** 12个月（2024年8月1日-2025年7月31日）,服务空档期（即2024年8月1日至开始提供服务之前)由原供应商（2023年供应商）按照2024年需求提供服务，期间产生的费用由投标人，按照实际服务时间及2024年合同单价与原供应商按实结算。

**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；

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8月23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8月23日09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8月23日09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：杭州市公安局交通警察支队

地 址：杭州市文晖路336号

传真： /

项目联系人（询问）：蒋斌

项目联系方式（询问）：87282217

质疑联系人：郑红军

质疑联系方式： 87282209

2.采购代理机构信息

名称：浙江信达咨询监理有限公司

地址：杭州市德胜路289号602；

传 真： /

项目联系人（询问）： 沈州

项目联系方式（询问）：13666623146

质疑联系人： 吴秀琴

质疑联系方式：1358800576

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、钟先生，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：2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务，属于软件和信息技术服务行业；中小企业划分标准为：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**安全加固及应用迁移改造服务、城市货运导航数据运营服务**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，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：杭州市德胜路289号602室；备份投标文件签收人员联系电话：沈州13666623146。**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 | **招标服务费** | 采购代理机构代理服务费用：  中标人需向浙江信达咨询监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，根据《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40%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。 |

**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人由政采云平台随机抽取相关专业抽取产生）】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。采购人成立验收小组（验收小组由5人组成：其中采购人1名，从政采云政企区专家库抽取相关专业专家4名），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**

（一）项目概况

租赁内容：本项目以购买服务方式，提供交通管理数据全生命周期运营服务、安全加固及应用迁移改造服务、货运导航数据及运营保障服务、安全防控风险预警服务，要求提供不少于11人驻点服务。

实施目标：通过本项目实施，提供常态化交通数据运维服务，为采购人正常业务运行提供数据支撑、模型支撑、技术保障支撑，完成采购人数据及应用安全迁移改造，实现数据及应用安全合规。

租赁期：12个月（2024年8月1日-2025年7月31日）,服务空档期（即2024年8月1日至开始提供服务之前)由原供应商（2023年供应商）按照2024年需求提供服务，期间产生的费用由投标人，按照实际服务时间及2024年合同单价与原供应商按实结算。

（二）预算金额：867.45万元（其中2024年安排346.98万元）；最高限价：854.4500万元

（三）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（）

（四）采购标的是否进口产品：🞎进口🞎国产，本项目为服务采购。

（五）拟采购标的的技术要求

**一）项目服务内容（标\*项参数投标时提供第三方检测机构出具的具备CMA标识的检测报告）**

**（一）交通管理数据全生命周期运营服务**

1、专网云平台系统运行及数据治理

（1）数据接入服务

将各类信息化系统的结构化、半结构化、非结构化多种类型数据统一接入和预处理，预计接入30多张相关数据库表，每日接入数据量在5.2亿条左右，每日约100GB 。

1）接入杭州市机动车卡口过车数据；

2）接入互联网实时交通数据，包含交通事件、拥堵预警等；

3）根据要完成表单的接入工作，每月底提供数据接入清单。

（2）数据加工治理服务

1）数据探查服务：对接入的杭州市机动车卡口过车、交通工程、互联网实时交通等多种类型数据来源进行打标。通过对来源数据存储位置、提供方式、总量和更新情况、业务含义、字段格式和取值分布、数据结构、数据质量等属性进行多维度探查，完成数据识别工作（例如空值率、值域及分布、命名实体、问题数据等多维度探查识别），为数据定义提供依据。

2）数据读取服务：在完成数据探查及数据定义工作后，将杭州市机动车卡口过车、交通工程、互联网实时交通等源数据与数据定义进行对比核验，确保数据质量和准确性。同时，对各种异构数据进行解密、解压、适配等多个环节操作，并对数据进行字符集转换、半结构化数据转换等其他转换，使数据符合数据处理要求的格式，供下一步处理。

3）数据清洗服务：按照数据清洗标准进行杭州市机动车卡口过车、交通工程、互联网实时交通等100多张书库表数据过滤、去重、格转、校验等数据清洗操作，从而实现数据标准化，包括数据对标、数据去重、数据转换以及数据完整性校验、规范性校验、一致性校验等。

4）数据共享服务：以专网云平台数据资源池为数据底座，通过数据共享打通采购人各部门的数据壁垒，加速数据资源由业务需求驱动和聚集，在业务协同上起到数据融合和共用的作用。为交通局日常业务、市局大数据平台、路网运行等场景提供杭州市机动车卡口过车、交通工程、互联网实时交通等数据支撑

5）数据传输服务：在数据共享和分发过程中，将涉及到一条或多条链路，数据传输将维护数据传输链路安全畅通，保障数据在传输过程中不错、不重、不丢。

6）模型标准化：使用标准化标签设计模型，包括杭州市机动车卡口过车、交通工程、互联网实时交通等众多的数据统计模型、分析模型、监控模型均具备管理和维护标识，便于模型运行维护过程中的统一化和规范化。

7）任务管理：对数据接入过程进行可视化管理，浏览数据接入任务，修改接入任务配置、实时调配任务的资源，设定任务通知等相关内容，保障接入任务顺畅进行。

8）断点传续保障：通过断点记录、断点标识、断点恢复，保障数据在下载或上传时,将下载或上传任务进行切分,每一个部分采用一个线程进行上传或下载,如果碰到网络故障,保障从已经上传或下载的部分开始继续上传下载未完成的部分，确保数据不重复、不缺失，从而提升数据传输效率、提高数据传输稳定性、减少网络带宽占用。

（3）数据透出服务

数据透出开发：按照业务场景的数据需求，提供对应的数据开发服务，实现数据的共享。完成接口透出的开发，可用于进行路网运行、交通事件、交通需求、交通舆情等决策分析业务。

（4）数据统计服务

1）统计类数据开发服务：满足支队日常统计类业务保障，如拥堵统计、事故统计、警情统计等，并实现数字、excel、word等多样式统计结果呈现。

2）持续提供工程类、秩序类等的数据模型、算子模型开发工作，预计开发模型200个。

（5）运营服务

对开发完成的数据魔方等进行运营保障工作。

监测类数据工作：满足支队日常监测类业务保障，如在途量监测、拥堵指数监测、平均速度监测及某重点路段、重点路口拥堵监测等。同时，结合监测类数据接口开发，为采购人的大脑2.0各应用平台提供监测运营保障，每天巡检，每周出具运行监测报告一份。

（6）专网云平台运行保障

针对专网云平台运行提供驻点服务和应急响应，保障平日系统云资源的规划、开通、监测和运营保障。在重大活动和重大节日期间，提供云平台的应急保障。每天巡检，每天出具城市大脑云平台运行监测报告一份。

2、公安网数据治理

（1）数据上云服务

1）数据源管理：对数据接入的源端和目的端进行基本信息维护，提供对接入组件内数据源统一操作管理的能力，支持根据数据源名称搜索数据源，支持各种异构数据源的新增、编辑、删除等操作。

2）数据探查：以可视化配置的形式提供对数据的探查功能，包括数据接入方式探查、业务探查、字段探查、数据项集探查、问题数据探查等，可用于对来源数据存储位置、提供方式、总量和更新情况、取值分布、数据质量等进行多维度探查，以达到认识数据的目的，预计完成约200张表的数据探查工作，主要包括在专网经过初步治理后的数据、以及市局大数据平台中和采购人业务强相关的部分数据。

3）数据定义：包括数据分级分类定义、数据提取策略定义等步骤。按照部标GA/DSJ 230-2019和GA/DSJ 231-2019规范，定义数据项的字段性质分类和字段敏感度分类；对结构化/半结构化数据提取策略进行定义，实现来源数据资源/数据项到目的数据资源/数据项的提取映射关系，为数据治理提供依据。

4）数据读取：建立跨网络、跨平台的数据安全接入通道，为内部及存在信息共享的部门间数据抽取汇聚提供接口通道，支持多源异构数据的源系统读取数据，包括文件读取、数据库读取及服务接口读取等，预计完成约200张表的数据读取工作，主要包括在专网经过初步治理后的数据、以及市局大数据平台中和采购人业务强相关的部分数据。

（2）数据治理服务

1）数据清洗：按照数据清洗标准进行数据过滤、去重、格转、校验等数据清洗操作，从而实现数据标准化，包括数据对标、数据去重、数据格转、数据校验等，预计完成约200张表的数据清洗工作。

2）数据关联：根据数据定义中的关联规则或算法，将数据和其它知识数据、业务数据等进行关联，并输出关联信息，包括关联回填、关联提取。

3）数据提取：按照数据标准进行字段映射提取和处理函数配置，实现对源数据中各类数据的关键信息提取，预计完成约200张表的数据提取工作。

4）数据分发：通过数据分发，实现对提取、清洗、关联、比对和标识后的数据进行分发处理（如：将结果数据对应分发到原始库、资源库等），预计完成约200张表的数据分发工作。

（3）数据开发服务

1）数据指标服务：包括指标计算、指标推送、指标采集；

2）指标计算：基于客户需求完成指标内容的开发，整体流程包括：指标数据对接、指标详细设计、指标代码实现等，预计完成约50类的指标计算工作。

3）指标推送：基于指标注册的更新频率要求将指标结果推送到指标中心，以可视化配置的形式对指标推送任务进行管理，同时支持以查看日志的形式对历史推送情况进行验证，预计完成约50类的指标推送工作。

4）指标采集：指标推送是从指标中心推送指标结果，而指标采集是从指标中心将指标结果进行采集，采集的范围可以根据采购人的实际使用需求进行申请；将指标结果从指标中心进行采集之后可以用于采购人相关业务系统的应用，预计完成约20类的指标采集工作。

5）数据融合服务：支撑客户特殊的数据使用需求，包括：数据关联、数据融合等，生成特定的结果表数据可以用于后续数据建模、数据查询、数据透出等数据使用需求，方便业务使用的同时也可以在数据安全层面进行把控，预计完成约20项的数据融合工作。

6）计算分析服务：基于特定需求完成计算逻辑设计，针对云上已交付的数据治理成果开展统计分析并产出计算结果，满足客户数据分析需求，预计完成约20项的计算分析工作

7）进行现有200类数据魔方业务模型的梳理工作；在数据域进行200类数据魔方模型的重新设计、重新构建等工作（由于视频专网上的数据魔方模型不能直接迁移到数据域，故需要在数据域中将视频专网的里面的魔方重新在进行搭建并维护；因视频专网和数据中的数据存在一定的差距，且为了提升模型的多用途、计算等能力，故进行重构），涉及到的模型包括每日交通量、道路速度统计查询、高峰延误指数、道路早晚高峰速度模型等；实现重构200类数据魔方模型的测试、运行、优化等工作

8）根据业务发展以及云上数据治理需要，新增50个业务类、服务类等相关模型的设计、开发、测试、运营、优化等工作，涵盖交通卡口流量统计模型、卡口间车流OD统计模型等模型。

（4）数据能力支撑

1）数据资源管理：包括资源市场、资源档案、资源审批；

2）资源市场：按照统一的标准规范对数据资源进行管理，实现数据资源科学、有序、安全使用。

3）资源档案：对数据资源进行档案式管理，使的用户更方便地了解和使用数据资源，简化用户认知数据表的难度，提高数据易用性。

4）资源审批：提供资源审批功能供民警进行合理性验证，同时，以线上资源审批工单的形式进行管理，方便后续进行溯源管理。

预计完成200张表的资源的注册与管理工作。

5）服务资源管理：包括服务市场、服务安全。

6）服务市场：以界面化的形式进行表转服务的注册，已发布的数据服务将展示在服务市场中供业务方申请使用。

7）服务安全：以数据应用的身份对服务接口进行白名单权限认证，支持对服务接口进行调用限额，避免单应用的异常调用影响整体系统。

预计完成30个服务的注册与管理工作。

8）数据推送服务：数据推送服务主要用于支撑采购人内部系统在云上的数据使用需求，包括离线数据推送、实时数据推送；

9）离线数据推送：离线数据推送指的是将上云或治理完成的结果表推送到应用方特定的关系型数据库，预计完成50张表的离线数据推送。

10）实时数据推送：实时数据指的是将实时数据推送到应用方的datahub，用于满足应用方的实时数据使用需求，预计完成30张表的实时数据推送。

11）数据透出服务：数据透出服务用于支撑采购人对外的数据共享需求，主要针对历史共享数据清单的数据链路进行梳理与切换，预计完成50张表的数据透出工作。

12）能力中心对接，包括指标中心对接、IT服务平台对接。

13）指标中心对接：包括指标推送与指标采集：指标推送是将采购人的相关系统、模型的成果转化为指标服务，发布到指标中心；指标采集是将指标中心各个业务系统和大屏已经开发好的指标成果进行采集共享，避免重复开发。

14）IT服务平台对接：对接IT服务平台注册的相关服务接口，通过服务接口可以查询其它部门共享的业务系统数据，满足采购人特定的数据使用需求。

（5）数据预警运营

1）上云任务监控运营：对接入组件的运行状况做一个整体的监控、包括任务监控、事件通知以及节点监控，通过监控中心发现任务或者执行节点的异常信息，及时预警通知运营人员，及时解决，预计需要完成400+个接入任务的运营管理。

2）治理任务监控运营：将当前数据治理组件中的异常预警按照预警时间的倒序来进行展示，提供预警时间、处理状态、预警级别、监控对象、预警类型五种筛选条件来对预警进行分类，方便运营人员快速定位并修复数据治理问题，保障数据稳定性，预计需要完成200+个治理任务的运营管理。

3）针对已经完成的200+数据模型和魔方算子进行维护、升级、运营等工作。

**（二）安全加固及应用迁移改造服务**

1、网络安全服务

针对采购人公安网、车管专网与视频专网的现状，公安网的网络安全性能尚能满足现有业务的安全保障工作。视频专网内仅建设有网络安全网关与大量的边界防护设备，网络内部安全隐患较大，故本期着重针对视频专网进行安全保障服务。

（1）漏洞扫描服务

安全漏洞检测是脆弱性识别的重要手段，能够发现设备和系统中存在的风险点，分析技术措施的有效执行，了解漏洞的危害，通过及时修补完善，避免对信息系统造成严重影响。

采用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，扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提供准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案，协助采购人进行解决。

（2）数据库审计服务

以安全为核心的审计服务，以全面审计和精确审计为基础，通过全面管理手段贯穿安全事件处理生命周期，致力于全面降低安全风险。通过全面审计，深入了解安全事件的多层次方面，包括对潜在威胁的深入分析和对系统漏洞的详尽检查，确保系统在安全方面的高度韧性。强调精确审计，通过高度精细的审计过程，发现并识别任何异常活动，包括微小的安全漏洞和未经授权的访问，有效地防范潜在风险。全面管理贯穿整个安全事件处理生命周期，建立起强大而可持续的安全框架，包括对安全策略的不断优化和更新，以适应不断演变的威胁环境。这项审计服务不仅仅关注技术层面的保障，更注重整个组织的安全文化建设。通过构建的审计服务，实现了全面降低安全风险的目标，为采购人提供持久而可靠的安全保障。

（3）日志审计服务

通过对网络设备、安全设备、主机和应用系统日志进行全面标准化处理，实现一个高效的安全监控体系。通过及时发现各类安全威胁和异常行为事件，以保障采购人业务的持续、安全运营。通过标准化处理各种日志信息，建立一个有机的关联体系，使得管理人员能够从全局的视角深入了解系统运行状态，确保任何潜在威胁都不会对业务造成中断。

基于国际标准的关联分析引擎服务工具，提供全维度、跨设备、细粒度的关联分析，通过透过事件表象还原事件背后的信息，提供真正可信赖的事件追责依据，为业务运行的深度安全提供坚实支持。实现信息资产的统一管理和监控资产的运行状况，提供集中化的统一管理平台工具。完成所有的日志信息集中收集与处理。

通过对整体安全状况的全面审计，在第一时间发现潜在的问题并采取相应的措施。服务通过标准化处理日志信息，确保系统中的各类信息得到规范、统一的管理。通过关联分析引擎服务工具，深入挖掘事件背后的信息，为管理人员提供更为全面的安全视角。

（4）安全运营服务

提供1名专业安全服务人员配合采购人开展安全运营管理工作，提供5\*8小时服务，负责公安信息网、视频专网、电子政务外网等相关网络的安全运营管理工作。协助开展网络安全主管部门安全检查，协助开展等级保护定级、备案、建设整改、测评和监督检查等。

网络安全技术防护策略持续改进主要针对日常安全监测和安全风险检查的结果进行综合分析研判，识别网络安全威胁和脆弱性，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，并定期开展策略配置备份、系统软件、特征库升级等操作。

定期针对日常安全监测和安全风险检查的结果进行综合分析研判，识别网络安全威胁、脆弱性和不合规配置项，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，以持续提升安全运行和防护能力。

（5）应急响应服务

应急响应服务通常包括采取远程、现场等紧急措施和行动，恢复业务到正常服务状态；调查安全事件发生的原因，避免同类安全事件再次发生；在需要司法机关介入时，提供法律认可的数字证据等。

安全专家采取远程、现场等方式应对采购人突发的安全事件和安全问题。专家通过事件分析、原因查找、事件处置、证据保留、及事件溯源等方式，快速解决采购人信息安全事件及问题，恢复业务及系统的安全运行，并确保所有事件应急处置过程得到有效控制和记录。

当需要应急响应协助采购人针对应用系统发生安全事件，并产生重大影响时，提供应急资源支持和应急人员支持，评估影响范围、事件抑制、溯源分析和复盘安全事件，协助开展业务恢复工作，并针对安全事件提供有效的整改意见。每年提供不少于4次应急响应服务。

（6）高级渗透测试服务

渗透测试服务是安全专家通过利用目标应用系统的安全弱点，模拟黑客可能使用的攻击方法和漏洞发现技术，以人工渗透为主，漏洞扫描工具为辅，在保证整个渗透测试过程都在可以控制和调整的范围之内，尽可能的获取目标信息系统的管理权限以及敏感信息的过程。

通过真实模拟黑客使用的工具和分析方法对采购人指定的信息系统进行模拟攻击，结合智能工具扫描结果，由网络安全高级专家进行深入的手工测试和分析，旨在识别工具弱点扫描无法发现的问题。这一过程包括先进的渗透测试工具的运用，模拟各类攻击场景，全面评估系统对于潜在威胁的抵抗能力。手工测试和分析与智能工具扫描相结合，通过深入的测试，发现那些仅依靠工具难以察觉的问题，提高对系统安全性的全面把控。服务注重发现系统中存在的潜在问题，如未经授权的访问、敏感数据的泄漏等，并为每个问题提供详尽的反馈和加固建议，确保信息系统能够在未来面对各类安全挑战时更为坚固和可靠。通过全面的、深度的渗透测试将为采购人信息系统提供实用而有效的安全加固方向，确保其在不断演进的网络威胁环境中保持最佳的安全状态。每年提供不少于20个系统的渗透测试服务。

（7）应急预案服务

为了保障应急响应的服务质量，提供修订、完善应急预案服务。协助建立健全应急响应组织以及预防、预警机制，针对信息系统特点和可能的突发性安全事件拟制规范的应急处理流程，落实物质条件、人力和技术支撑等保障措施，制定出规范、全面、体系化的应急预案。

应急预案的制定和完善将规范应急处理行为，避免应急处理过程中出现混乱、无序状况，减少处理过程中错误的发生，从而避免不必要的损失。

（8）应急演练服务

应急演练服务根据国家、行业等相关规章和标准，结合近年发生的安全事件和面临的安全风险，对采购人的网络安全应急预案进行全面评估与修订。基于符合采购人自身组织架构的网络安全应急预案服务，明确各个部门的责任，准备措施以及应对突发事件的配合机制，提供特定场景的安全演练。

根据采购人需求提供特定场景的演练，可选形式：桌面演练、现场演练。桌面推演服务包括：演练场景分析、演练剧本编写、现场调研、人员组织等。现场演练服务内容包括：现状调研、演练方案编制、演练流程编制、现场演练组织、演练总结等。通过应急演练有效检验并完善应急预案、应急流程，提升采购人人员整体应急能力。

（9）重要时期安全专家保障服务

在重要时期，网络安全保障服务在重大活动的前、中、后阶段发挥着至关重要的作用。服务涵盖活动前的安全自查和运维，活动中的日志分析、安全值守、应急响应等，以及活动后的复盘总结。通过真实模拟黑客攻击手段，结合智能工具扫描和深入的手工测试与分析，专业团队识别工具弱点扫描难以发现的问题。这一全方位的服务体系致力于全面提升活动相关网络的安全性，增强网络的防御能力，以为采购人提供安全、快速、有效的安全服务。早期的安全自查和运维消除潜在隐患，实时的分析和值守保障网络安全，而活动后的复盘总结提供宝贵经验教训，不断优化服务流程。这一综合性的服务策略为重要时期的活动提供了强有力的网络支持，确保其在安全、稳定的网络环境中顺利展开，最大程度地降低潜在风险。每年提供不少于4次保障服务并提供安全日报。

（10）跨网数据请求与响应服务

提供跨网数据请求与响应工具，为系统和用户在异构网络环境下实现了高度灵活而无缝的数据交流能力。通过协议适配，服务克服了不同网络通信障碍，确保数据在不同网络之间的顺畅传输。安全性需得到充分保障，采用先进的加密技术、身份验证和访问控制，有效预防未经授权的访问和数据泄露。服务通过优化性能，包括对数据传输通道的优化、带宽管理和网络流量的控制，确保了高效、快速的数据交换；提供适当的错误处理机制，能够及时检测并解决问题，保障数据交流的连续性和稳定性；通过引入校验和机制，确保在数据传输过程中不会发生数据损坏或篡改。

（11）数据交换边界防护服务

提供数据交换边界防护服务工具，在采购人视频专网与公安网业务进行数据交换过程中，提供数据的机密性、完整性和可用性的服务，保护数据在跨网传输和通信过程中的安全。在网络边界部署边界防护工具，对进行细粒度的访问控制。对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；拥有细粒度为端口级，并根据会话状态信息为数据流提供明确的允许/拒绝访问处理，可将会话处于非活跃一定时间或会话结束后终止网络连接并通过限制网络最大流量数及网络连接数以提升安全等访问控制能力。

（12）违规外联监测服务

引入先进的监测技术和安全审计工具，实时监测网络流量、检测异常访问和识别不寻常的数据传输模式，以主动发现违规外联行为，提高对潜在威胁的感知。建立快速响应机制，一旦检测到异常行为，立即向本级监管方报告，以便迅速采取应对措施，增强监管方对整个网络系统的掌控。完成监测系统的定期检查和更新，修复系统漏洞，升级防护机制，保持系统的健康状态。采用智能化的边界安全防护系统，通过深度学习和行为分析，系统能够学习并识别正常的网络活动模式，实现对异常行为的自动识别和响应。

2、关键业务安全迁移及改造

2.1合成作战应用迁移服务

提供交管专有云平台合成作战应用向警务云迁移改造服务，满足信创要求，包括人车查询、电动车智控、勤务管理、视频巡查、预警中心、警情打标等模块迁移改造。投标人应保证在服务期内完成该项服务，具体内容如下：

（1）人车查询模块。包括机动车信息查询、驾驶人信息查询，具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、整体系统调试及优化。

（2）电动车智控PC端。电动自行车智控闭环应用根据设定的违法查处、撤控规则，并串联移动端查处应用，支撑违法处置高效开展，绩效考核准确快捷。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（3）勤务管理模块。包含巡防区管理、勤务智检、在线警力、勤务排班等功能。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（4）视频巡查PC端。包括视频巡查处置流程及视频巡查驾驶舱展示。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（5）预警中心。应用对接多个第三方平台数据包括过车、违法等数据，直接预警或通过模型和算法产生预警。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（6）警情打标模块。包括标签设置、标签项自定义、警情打标、查案打标、标签筛选、相关统计、打标导出详情等功能。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、整体系统调试及优化。

2.2非现场执法平台升级改造服务

提供支队非现场执法平台软件迁移改造服务，满足信创要求，包括软件服务以及硬件支撑环境搭建服务。投标人应保证在服务期内完成该项服务，具体内容如下：

（1）提供软件服务，包括非现场平台功能迁移、特色需求优化迁移、平台数据对接和扩容、平台业务接口迁移、专网数据转发、非现场功能升级等服务，构建公安网环境下的支队非现场执法平台，支撑非现场业务的高效运转。

1）非现场平台功能迁移服务：主要涉及将现有非现场执法平台的所有功能迁移至新的软件平台。这包括但不限于数据采集、处理、存储、查询和分析等功能的完整迁移。

2）特色需求优化迁移服务：由于业务需求可能存在差异，因此需要进行特定的优化以满足采购人特色需求。包括优驾容错功能的优化、急事通功能的完善等。

3）平台数据对接和扩容服务：在迁移过程中，需要确保新旧平台之间的数据无缝对接，同时考虑到未来数据增长的需求，进行必要的扩容准备，以支撑更大规模的数据处理和分析。

4）平台业务接口迁移服务：对于与外部系统或应用之间的业务接口，需要进行相应的迁移，以确保与外部系统的兼容性和数据交互的顺畅性。

5）专网数据转发服务：在视频和专网采集的非现场数据，统一经过安全边界摆渡至公安网侧。

6）非现场功能升级服务：根据中国信息安全评测中心发布的《安全可靠测评工作指南》要求，需要对非现场执法平台的功能进行升级和改进。涉及到使用国产信创产品来构建新的平台，以满足公安网环境下对数据安全和隐私保护的高标准要求。

（2）支队非现场执法平台硬件支撑环境搭建服务：租赁设备生产日期要求为2024年1月1日以后生产，项目服务期结束后设备处置权归投标人所有；

|  |  |  |
| --- | --- | --- |
| 序号 | 服务 | 参数 |
|  | 部署4台物理服务器用于视频专网环境中违法终端设备的对接与数据上传 | 处理器：≥16核 2.5G\*1  内存：≥DDR4 32G\*2  硬盘：≥960G SSD硬盘\*2 +4×600G SAS硬盘  网络：≥双口万兆网卡（含模块）  电源：≥550W电源模块\*2  详细参数见“视频专网单台服务器详细参数要求” |

视频专网单台服务器详细参数如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **一级性能参数指标** | **二级性能参数指标** | **指标要求** |
| 1 | ▲CPU规格 | ▲CPU 信息 | （1）配置国产架构处理器，支持超线程技术和睿频技术； |
| 1. 单颗CPU物理核心数≥16核、主频≥2.5GHz、末级缓存容量≥32MB、线程数≥32、热设计功耗≥135W、支持内存的最高速率≥3200MHz、通道数≥4、位宽≥64位；   供应商应在投标时给出CPU型号； |
| 2 | ▲主板规格 | ▲主板支持的CPU 和内存情况 | 主板支持CPU ≥2颗，内存数量支持≥ 16个；  供应商应在投标时给出主板支持的CPU型号； |
| 3 | ▲主板内存槽数量 | 主板内存槽数量≥16个 |
| 4 | ▲主板存储接口 | （1）前置可支持≥12个SATA/SAS/NVME盘；后置可支持 2 SATA/SAS |
| （2）板载内置≥1个M.2 SATA插槽； |
| 5 | ▲PCIe 插槽接口 | 符合 PCIe3.0 或以上的高速串行计  算机扩展总线标准，PCIe 的接口速  率与位宽需保证向下兼容 |
| 6 | ▲主板 PCIe 插槽数量及规格 | PCIe 插槽数量≥5个,  1个PCle4.0 x16插槽 (x16 Lane)  3个PCle4.0 x8插槽 (x8 Lane)  1个PCle4.0 x4插槽 (x4 Lane)  可通过扩展卡进行插槽扩展 |
| 7 | ▲内存规格 | ▲内存数量 | 内存数量≥4 |
| 8 | ▲内存规格 | 实配≥64GB DDR4 |
| 9 | ▲内存通道 | 支持≥4个内存接口通道 |
| 10 | ▲存储规格 | ▲硬磁盘实配容量 | 实配硬磁盘≥2.4T，实配固态盘≥1.92T； |
| 11 | ▲硬盘实配数量 | 实配硬磁盘≥4块600G 2.5寸 10K 12Gb SAS硬盘，实配固态盘≥2块960G 2.5寸 SATA 6Gb R SSD； |
| 12 | ▲硬盘插槽数量及规格 | （1）最高支持≥12个SATA/SAS/NVME 3.5寸/2.5寸硬盘 |
| （2）后置可支持≥2个SATA/SAS 2.5寸硬盘/3.5寸硬盘； |
| 13 | ▲网络规格 | ▲网口速率和数量 | ≥1个双口万兆网卡（含模块） |
| 14 | ▲外部接口规格 | ▲显示接口 | 配置≥1个VGA接口 |
| 15 | ▲USB 接口 | 配置≥4个USB3.0接口，2个位于机箱后部，2哥位于机箱前部。 |
| 16 | ▲电源规格 | ▲电源模块数量 | ≥2 |
| 17 | ▲电源功率 | ≥550W，电源模块功率应有一定冗余， 满足处理器满载时的需求 |
| 18 | ▲整机规格 | ▲外观和结构 | a)服务器的零部件应紧固无松动，可插拔部件应可靠连接，开关、按钮和其它控制部件应灵活可靠，布局应方便使用； |
| b) 产品表面不应有明显的凹痕、划伤、裂缝、变形和污染等。表面涂层均匀，不应起泡、龟裂、脱落和磨损，金属零部件无锈蚀及其它机械损伤； |
| c) 产品表面说明功能的文字、符号和标志应清晰、端正且牢固； |
| d) 应在服务器的显著位置提供运行状态的指示功能，并在随机文件中明确具体含义； |
| e) 机架、机箱的尺寸应符合通用机柜的安装要求，插入总线插座的电路板接口外形尺寸应符合有关总线标准的规定，将机箱固定在机柜上，机箱底面最大下垂变形不得干涉相邻机体； |
| f) 高密度服务器应给出 CPU 个数与机柜高度； |
| g) 服务器尺寸具体要求在随机文件中明确 |
| 19 | ▲尺寸（高×宽×深） | 供应商应在投标时给出产品尺寸； |
| 20 | ▲环境适应性 | 气候环境适应性应符合 GB/T9813.3 的有关规定，工作温度 10～35℃，贮存运输温度-40～55℃；工作相对湿度 35%～80%，贮存运输相对湿度 20％～93%（40℃）；大气压86～106kPa |
| 21 | ▲机械环境适应性 | 机械环境适应性应符合 GB/T9813.3 的有关规定 |
| 22 | ▲噪声 | 符合 GB/T 9813.3 的有关规定，在产品说明中给出具体测试值塔式服务器噪声在空闲状态下不大于 50dB |
| 23 | 机柜规格 | ▲机柜尺寸 | 供应商在投标时给出长度、高度和深度； |
| 24 | ▲主板 | ▲主板外部接口种类 | 支持 USB、显示、管理等接口,如VGA、USB3.0接口、BMC 管理端口 |
| 25 | ▲网络功能 | ▲网络功能 | 支持网络连接、网络访问、数据交换和网络管控功能 |
| 26 | ▲CPU功能 | ▲计算处理 | 支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，处理器与存储部件、网络部件、I/O部件等组成计算系统，提供数据处理、网络接入等计算相关功能 |
| 27 | ▲密码算法实现 | CPU 芯片应符合 GM/T 0008 的相关规定，或芯片密码模块应符合 GB/T37092 或 GM/T 0028 的相关规定 |
| 28 | ▲电源功能 | ▲电源热插拔 | 整机电源模块应具备热插拔功能 |
| 29 | ▲电源过流保护 | 支持过流及短路保护的功能 |
| 30 | ▲整机功能 | ▲散热方式 | 支持风冷散热方式 |
| 31 | ▲管理系统功能 | ▲BMC 固件基础功能 | 1) 支持 DHCP 设置网络功能；  2)支持静态 IP 设置网络功能；  3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能；  4)支持日志信息导出和记录删除功能；  5)支持通过管理接口向外输出准确的报警信息功能；  6)设备的 BMC 管理软件应能够按报警的严重程度进行区分；  7)支持 IPMI2.0、SNMP 或 Redfish等接口功能；   1. 支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能；   9)支持基于网络开启、关闭和重启设备的功能，并查询当前设备开机运行状态；  10)支持故障提示功能，并可通过接口读取服务器故障信息；  11)支持基于网络的固件更新功能，包括 BMC 和 BIOS 等；  12)支持基于网络安装操作系统的功能，并可通过网络控制台访问设备；  13)支持通过本地的硬盘或光驱等存储设备，基于网络完成设备的操作系统安装功能；  14)支持通过浏览器打开管理界面并登录功能；  15)支持设置口令策略功能；  16)支持访问权限设置功能，并通过日志记录访问事件；  17)支持对出厂默认的用户名及口令进行安全保护功能，并提供默认口令修改提示；  18)支持读取设备主板的工作环境温度功能；  19)支持读取服务器 CPU 等核心器件的温度功能；   1. 支持通过外部管理工具进行 BMC参数设置的功能，并可基于网络通过外部管理工具对 BMC 进行管理； 2. 应支持固件版本查询、固件升级   22)支持基于网络实现开关机和复位控制的功能；  23)BMC 启动时间应不超过 180s，实现功能包括网络、IPMI、散热、传感器服务可用；  24)支持 BMC 固件设置的恢复出厂功能 |
| 32 | ▲BIOS 固件基础功能 | a）支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能；  b）支持上电初始化界面显示 CPU 信息、内存信息、固件版本和部分快捷键信息功能；  c）支持设置界面中英文显示切换功能；  d）支持查看 PCIe 设备信息，SATA设备信息功能；  e）支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口；  f）支持设置启动顺序，并按照设置的启动顺序启动功能；  g）支持安全启动功能；  h）支持设置口令、修改口令、验证口令功能；  i）支持板载显示控制或独立显卡的显示控制功能；  j）支持 RAID 识别和启动功能；k）支持串口重定向功能；  l）支持固件更新功能；  m）支持 BIOS 固件设置的恢复出厂功能；  n）支持网络引导启用和关闭功能 |
| 33 | ▲远程控制 | 支持远程关机和重新启动功能 |
| 34 | ▲操作系统及驱动功能 | ▲操作系统及驱动的升级 | 支持通过网络、闪存盘对操作系统、驱动进行升级 |
| 35 | ▲操作系统功能 | 支持访问控制、安全审计、网络接入鉴别等功能；  操作系统其他功能满足操作系统政府采购需求标准中加\*的指标要求 |
| 36 | ▲中文信息处理功能 | ▲中文信息处理 | 符合 GB 18030 的有关规定 |
| 37 | ▲关键部件安全要求 | ▲关键部件安全要求 | CPU 和操作系统等关键部件应当符合安全可靠测评要求 |
| 38 | ▲固件安全要求 | ▲故障检测 | 支持故障检测功能，可以检测到具体的 FRU（内存、硬盘等）的故障并发出告警 |
| 39 | ▲系统安全要求 | ▲弱口令字典检查 | 支持弱口令字典检查功能，出现在弱口令字典中的字符串不能被设置为用户口令 |
| 40 | ▲白名单访问控制 | 支持基于时间、IP 或 MAC 白名单访问控制 |
| 41 | ▲二次鉴别 | 支持二次鉴别功能。对于用户配置、权限配置、公钥导入等重要的管理操作，已登录用户应通过二次鉴别后，才能执行操作 |
| 42 | ▲密码证书安全加密存储 | 支持对带外管理系统中的用户口令和证书等敏感信息进行加密存储，禁止使用私有的和业界已知不安全的密码算法 |
| 43 | ▲敏感信息安全加密传输 | 支持使用安全的传输加密协议（如SSH 或 HTTPS 等）传输用户的敏感信息 |
| 44 | ▲信息安全要求 | ▲研发过程安全 | 供应商承诺，生产商已建立从需求、设计、开发、测试、维护端到端的开发流程管理机制，输出和保存开发流程中每个阶段的产品需求清单、设计文档、开发文档、测试记录等材料，保证各个流程可追溯； |
| 45 | ▲物理安全 | ▲物理安全 | 安全要求应符合 GB 4943.1 的规定 |
| 46 | ▲限用物质的限量要求 | ▲限用物质的限量要求 | 限用物质的限量应符合 GB/T 26572的要求 |
| 47 | ▲CPU性能 | ▲CPU 主频 | ≥2.5GHz |
| 48 | ▲单 CPU 核数 | ≥16 |
| 49 | ▲单 CPU 末级缓存容量 | ≥32MB |
| 50 | ▲内存性能 | ▲内存速率 | ≥3200MT/s |
| 51 | ▲电源能耗 | ▲电源能耗 | 符合 GB/T 9813.3 的有关规定 |
| 52 | ▲部件兼容性要求 | ▲内存兼容性 | 适配 3 种及以上厂商的内存产品，且均不低于产品支持的内存规格 |
| 53 | ▲固态存储兼容性 | 适配 3 种或以上厂商的固态存储产品，且均不低于产品支持的固态存储设备规格 |
| 54 | ▲网卡兼容性 | 网卡应适配两种或以上厂商产品 |
| 55 | ▲功能卡兼容性 | 内置或适配符合 PCIe 的功能卡，如：网络功能卡、存储功能卡及图形显示功能卡 |
| 56 | ▲外设兼容性 | ▲外设兼容性 | 兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB 光驱及 KVM 等，要求使用不同厂商的外部设备时，系统均能正常识别和安装驱动 |
| 57 | ▲软件兼容性 | ▲数据库兼容 | 兼容3个及以上厂商的数据库产品； |
| 58 | ▲中间件兼容 | 兼容3个及以上厂商的中间件产品； |
| 59 | ▲平台软件兼容 | 兼容3个及以上厂商的大数据平台； |
| 60 | ▲整机可靠性要求 | ▲整机可靠性 | m1 值（MTBF 的不可接受值）≥100000h； |
| 61 | ▲风扇可靠性 | 风扇寿命≥ 100000h |
| 62 | ▲部件可靠性 | 支持硬盘、电源、风扇热插拔 |
| 63 | ▲包装及运输要求 | ▲标志、包装、运输和贮存 | 符合 GB/T 9813.3 和商品包装政府采购需求标准的相关规定 |
| 64 | ▲服务响应 | ▲服务响应 | a) 提供电话、电子邮件、远程连接等多种形式服务；b) 提供同城 4h、异地 12h 技术响应服务，2 个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备；c) 建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务；d) 服务周期内提供产品的维修、换件和升级服务 |
| 65 | ▲培训服务 | 供应商提供培训材料、产品手册、培训视频等培训相关内容 |
| 66 | ▲服务周期 | ▲服务周期 | a) 服务期内，提供服务（含换件和维修）； |
| b) 设备停产后继续提供质量保障服务（含备品备件），服务终止时间与最后一批设备交付时间间隔不低于 6 年； |
| c) 产品停止服务时间应提前 1 年告知客户； |
| d) 产品发布日期需在随机文件中明确 |
| 67 | ▲服务工具要求 | ▲工具要求 | 提供设置服务器硬件、辅助操作系统安装等功能的辅助工具和管理软件。且随附软件应具有合法授权或版权 |
| 68 | ▲驱动安装升级指引 | 提供出厂安装的配件所需的驱动程序，形式包括但不限于驱动光盘、驱动下载链接等。其他配件应提供指引 |
| 69 | ▲管理软件 | 具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能 |
| 70 | ▲增值服务 | ▲厂家升级产品软件与扩容服务 | 提供原厂级的部件/软件产品升级和扩容能力 |
| 71 | ▲提供上门服务 | 具备提供上门服务的能力(可收费) |
| 72 | ▲供应链质量 | ▲抗干扰性 | 当产品部件出现供应风险时，应通知客户并提供风险应对方案确保产品的服务保障，必要时应停止相关受影响产品的销售 |
| 73 | ▲供应能力证明 | 供应商需提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货 |

|  |  |  |
| --- | --- | --- |
| 序号 | 服务 | 参数 |
|  | 部署4台高性能物理服务器器用于支撑改造后平台的搭建 | 处理器：≥2.2G 32C \*2；  内存：≥32GB DDR4 3200 RDIMM \*12；  硬盘：≥4TB 7.2k 6Gb \*4 + 960GB 6Gb R SSD \*3 + 960GB 6Gb M SSD \*1 + 480GB 6Gb R SSD \*2；  业务网口≥双口万兆网卡\*2（含模块）；  电源：≥800W电源模块\*2  详细参数见“高性能服务器详细参数要求” |

高性能服务器单台详细参数如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **一级性能参数指标** | **二级性能参数指标** | **指标要求** |
| 1 | ▲CPU规格 | ▲CPU 信息 | （1）配置2颗国产架构处理器，支持超线程技术和睿频技术； |
| （2）单颗CPU物理核心数≥32核、主频≥2.2GHz、末级缓存容量≥64MB、线程数≥64、热设计功耗≥220W、支持内存的最高速率≥3200MHz、通道数≥8、位宽≥64位；  供应商应在投标时给出CPU型号； |
| 2 | ▲主板规格 | ▲主板支持的CPU 和内存情况 | 主板支持CPU ≥2颗，内存数量支持≥32个；  供应商应在投标时给出主板支持的CPU型号； |
| 3 | ▲主板内存槽数量 | 主板内存槽数量≥32个 |
| 4 | ▲主板存储接口 | （1）前置可支持≥12个前置热插拔3.5硬盘或24个2.5硬盘，支持SAS/SATA/NVMe SSD  （2）板载可支持≥8个U.2 NVMe SSD  （3）板载可支持2个内置M.2 SSD，兼容PCIe 和SATA规格，支持2个SATA M.2组RAID  （4）后置可支持≥4个2.5寸硬盘，支持anybay  （5）后置可支持≥4个3.5寸硬盘，支持SAS/SATA/SSD |
| 5 | ▲PCIe 插槽接口 | 符合 PCIe3.0 或以上的高速串行计算机扩展总线标准，PCIe 的接口速率与位宽需保证向下兼容 |
| 6 | ▲主板 PCIe 插槽数量及规格 | 支持直插主板的riser方式扩展≥8个全高PCIe 4.0标准卡  支持1个直插主板的内置RAID卡PCIe标准插槽，不使用线缆连接，不占用后置PCIe标准卡槽位，可通过扩展卡进行插槽扩展 |
| 7 | ▲内存规格 | ▲内存数量 | 内存数量≥12 |
| 8 | ▲内存规格 | 实配≥384GB DDR4 |
| 9 | ▲内存通道 | 支持≥8个内存接口通道 |
| 10 | ▲存储规格 | ▲硬磁盘实配容量 | 实配硬磁盘≥16T，实配固态盘≥4.8T； |
| 11 | ▲硬盘实配数量 | 实配硬磁盘≥4块4TB 3.5寸 7.2K 12Gb SAS硬盘，实配固态盘≥3块960G 2.5寸 SATA 6Gb R SSD，≥2块480G 2.5寸 SATA 6Gb R SSD,≥1块960G 2.5寸 SATA 6Gb M SSD； |
| 12 | ▲硬盘插槽数量及规格 | （1）最高支持≥12个前置热插拔3.5硬盘或24个2.5硬盘，支持SAS/SATA/NVMe SSD |
| （2）后置支持≥4个2.5寸硬盘，支持anybay或后置支持≥4个3.5寸硬盘，支持SAS/SATA/SSD |
| 13 | ▲网络规格 | ▲网口速率和数量 | ≥2个万兆双口光纤网卡（含模块） |
| 14 | ▲外部接口规格 | ▲显示接口 | 配置≥1个VGA接口 |
| 15 | ▲USB 接口 | 配置≥4个USB3.0接口，2个位于机箱后部，2哥位于机箱前部。 |
| 16 | ▲电源规格 | ▲电源模块数量 | ≥2 |
| 17 | ▲电源功率 | ≥800W，电源模块功率应有一定冗余， 满足处理器满载时的需求 |
| 18 | ▲整机规格 | ▲外观和结构 | a)服务器的零部件应紧固无松动，可插拔部件应可靠连接，开关、按钮和其它控制部件应灵活可靠，布局应方便使用； |
| b) 产品表面不应有明显的凹痕、划伤、裂缝、变形和污染等。表面涂层均匀，不应起泡、龟裂、脱落和磨损，金属零部件无锈蚀及其它机械损伤； |
| c) 产品表面说明功能的文字、符号和标志应清晰、端正且牢固； |
| d) 应在服务器的显著位置提供运行状态的指示功能，并在随机文件中明确具体含义； |
| e) 机架、机箱的尺寸应符合通用机柜的安装要求，插入总线插座的电路板接口外形尺寸应符合有关总线标准的规定，将机箱固定在机柜上，机箱底面最大下垂变形不得干涉相邻机体； |
| f) 高密度服务器应给出 CPU 个数与机柜高度； |
| g) 服务器尺寸具体要求在随机文件中明确 |
| 19 | ▲尺寸（高×宽×深） | 供应商应在投标时给出产品尺寸； |
| 20 | ▲环境适应性 | 气候环境适应性应符合 GB/T9813.3 的有关规定，工作温度 10～35℃，贮存运输温度-40～55℃；工作相对湿度 35%～80%，贮存运输相对湿度 20％～93%（40℃）；大气压86～106kPa |
| 21 | ▲机械环境适应性 | 机械环境适应性应符合 GB/T9813.3 的有关规定 |
| 22 | ▲噪声 | 符合 GB/T 9813.3 的有关规定，在产品说明中给出具体测试值塔式服务器噪声在空闲状态下不大于 50dB |
| 23 | 机柜规格 | ▲机柜尺寸 | 供应商在投标时给出长度、高度和深度； |
| 24 | ▲主板 | ▲主板外部接口种类 | 支持 USB、显示、管理等接口,如VGA、USB3.0接口、BMC 管理端口 |
| 25 | ▲网络功能 | ▲网络功能 | 支持网络连接、网络访问、数据交换和网络管控功能 |
| 26 | ▲CPU功能 | ▲计算处理 | 支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，处理器与存储部件、网络部件、I/O部件等组成计算系统，提供数据处理、网络接入等计算相关功能 |
| 27 | ▲密码算法实现 | CPU 芯片应符合 GM/T 0008 的相关规定，或芯片密码模块应符合 GB/T37092 或 GM/T 0028 的相关规定 |
| 28 | ▲电源功能 | ▲电源热插拔 | 整机电源模块应具备热插拔功能 |
| 29 | ▲电源过流保护 | 支持过流及短路保护的功能 |
| 30 | ▲整机功能 | ▲散热方式 | 支持风冷散热方式 |
| 31 | ▲管理系统功能 | ▲BMC 固件基础功能 | 1) 支持 DHCP 设置网络功能；  2)支持静态 IP 设置网络功能；  3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能；  4)支持日志信息导出和记录删除功能；  5)支持通过管理接口向外输出准确的报警信息功能；  6)设备的 BMC 管理软件应能够按报警的严重程度进行区分；  7)支持 IPMI2.0、SNMP 或 Redfish  等接口功能；  8)支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能；  9)支持基于网络开启、关闭和重启设备的功能，并查询当前设备开机运行状态；  10)支持故障提示功能，并可通过接口读取服务器故障信息；  11)支持基于网络的固件更新功能，包括 BMC 和 BIOS 等；  12)支持基于网络安装操作系统的功能，并可通过网络控制台访问设备；  13)支持通过本地的硬盘或光驱等存储设备，基于网络完成设备的操作系统安装功能；  14)支持通过浏览器打开管理界面并登录功能；  15)支持设置口令策略功能；  16)支持访问权限设置功能，并通过日志记录访问事件；  17)支持对出厂默认的用户名及口令进行安全保护功能，并提供默认口令修改提示；  18)支持读取设备主板的工作环境温度功能；  19)支持读取服务器 CPU 等核心器件的温度功能；   1. 支持通过外部管理工具进行 BMC参数设置的功能，并可基于网络通过外部管理工具对 BMC 进行管理； 2. 应支持固件版本查询、固件升级   22)支持基于网络实现开关机和复位控制的功能；  23)BMC 启动时间应不超过 180s，实现功能包括网络、IPMI、散热、传感器服务可用；  24)支持 BMC 固件设置的恢复出厂功能 |
| 32 | ▲BIOS 固件基础功能 | a）支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能；  b）支持上电初始化界面显示 CPU 信息、内存信息、固件版本和部分快捷键信息功能；  c）支持设置界面中英文显示切换功能；  d）支持查看 PCIe 设备信息，SATA设备信息功能；  e）支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口；  f）支持设置启动顺序，并按照设置的启动顺序启动功能；  g）支持安全启动功能；  h）支持设置口令、修改口令、验证口令功能；  i）支持板载显示控制或独立显卡的显示控制功能；  j）支持 RAID 识别和启动功能；  k）支持串口重定向功能；  l）支持固件更新功能；  m）支持 BIOS 固件设置的恢复出厂功能；  n）支持网络引导启用和关闭功能 |
| 33 | ▲远程控制 | 支持远程关机和重新启动功能 |
| 34 | ▲操作系统及驱动功能 | ▲操作系统及驱动的升级 | 支持通过网络、闪存盘对操作系统、驱动进行升级 |
| 35 | ▲操作系统功能 | 支持访问控制、安全审计、网络接入鉴别等功能；  操作系统其他功能满足操作系统政府采购需求标准中加\*的指标要求 |
| 36 | ▲中文信息处理功能 | ▲中文信息处理 | 符合 GB 18030 的有关规定 |
| 37 | ▲关键部件安全要求 | ▲关键部件安全要求 | CPU 和操作系统等关键部件应当符合安全可靠测评要求 |
| 38 | ▲固件安全要求 | ▲故障检测 | 支持故障检测功能，可以检测到具体的 FRU（内存、硬盘等）的故障并发出告警 |
| 39 | ▲系统安全要求 | ▲弱口令字典检查 | 支持弱口令字典检查功能，出现在弱口令字典中的字符串不能被设置为用户口令 |
| 40 | ▲白名单访问控制 | 支持基于时间、IP 或 MAC 白名单访问控制 |
| 41 | ▲二次鉴别 | 支持二次鉴别功能。对于用户配置、权限配置、公钥导入等重要的管理操作，已登录用户应通过二次鉴别后，才能执行操作 |
| 42 | ▲密码证书安全加密存储 | 支持对带外管理系统中的用户口令和证书等敏感信息进行加密存储，禁止使用私有的和业界已知不安全的密码算法 |
| 43 | ▲敏感信息安全加密传输 | 支持使用安全的传输加密协议（如SSH 或 HTTPS 等）传输用户的敏感信息 |
| 44 | ▲信息安全要求 | ▲研发过程安全 | 供应商承诺，生产商已建立从需求、设计、开发、测试、维护端到端的开发流程管理机制，输出和保存开发流程中每个阶段的产品需求清单、设计文档、开发文档、测试记录等材料，保证各个流程可追溯； |
| 45 | ▲物理安全 | ▲物理安全 | 安全要求应符合 GB 4943.1 的规定 |
| 46 | ▲限用物质的限量要求 | ▲限用物质的限量要求 | 限用物质的限量应符合 GB/T 26572的要求 |
| 47 | ▲CPU性能 | ▲CPU 主频 | ≥2.2GHz |
| 48 | ▲单 CPU 核数 | ≥32 |
| 49 | ▲单 CPU 末级缓存容量 | ≥64MB |
| 50 | ▲内存性能 | ▲内存速率 | ≥3200MT/s |
| 51 | ▲电源能耗 | ▲电源能耗 | 符合 GB/T 9813.3 的有关规定 |
| 52 | ▲部件兼容性要求 | ▲内存兼容性 | 适配 3 种及以上厂商的内存产品，且均不低于产品支持的内存规格 |
| 53 | ▲固态存储兼容性 | 适配 3 种或以上厂商的固态存储产品，且均不低于产品支持的固态存储设备规格 |
| 54 | ▲网卡兼容性 | 网卡应适配两种或以上厂商产品 |
| 55 | ▲功能卡兼容性 | 内置或适配符合 PCIe 的功能卡，如：网络功能卡、存储功能卡及图形显示功能卡 |
| 56 | ▲外设兼容性 | ▲外设兼容性 | 兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB 光驱及 KVM 等，要求使用不同厂商的外部设备时，系统均能正常识别和安装驱动 |
| 57 | ▲软件兼容性 | ▲数据库兼容 | 兼容3个及以上厂商的数据库产品； |
| 58 | ▲中间件兼容 | 兼容3个及以上厂商的中间件产品； |
| 59 | ▲平台软件兼容 | 兼容3个及以上厂商的大数据平台； |
| 60 | ▲整机可靠性要求 | ▲整机可靠性 | m1 值（MTBF 的不可接受值）≥100000h； |
| 61 | ▲风扇可靠性 | 风扇寿命≥ 100000h |
| 62 | ▲部件可靠性 | 支持硬盘、电源、风扇热插拔 |
| 63 | ▲包装及运输要求 | ▲标志、包装、运输和贮存 | 符合 GB/T 9813.3 和商品包装政府采购需求标准的相关规定 |
| 64 | ▲服务响应 | ▲服务响应 | a) 提供电话、电子邮件、远程连接等多种形式服务；b) 提供同城 4h、异地 12h 技术响应服务，2 个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备；c) 建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务；d) 服务周期内提供产品的维修、换件和升级服务 |
| 65 | ▲培训服务 | 供应商提供培训材料、产品手册、培训视频等培训相关内容 |
| 66 | ▲服务周期 | ▲服务周期 | a) 服务期内，提供服务（含换件和维修）； |
| b) 设备停产后继续提供质量保障服务（含备品备件），服务终止时间与最后一批设备交付时间间隔不低于 6 年； |
| c) 产品停止服务时间应提前 1 年告知客户； |
| d) 产品发布日期需在随机文件中明确 |
| 67 | ▲服务工具要求 | ▲工具要求 | 提供设置服务器硬件、辅助操作系统安装等功能的辅助工具和管理软件。且随附软件应具有合法授权或版权 |
| 68 | ▲驱动安装升级指引 | 提供出厂安装的配件所需的驱动程序，形式包括但不限于驱动光盘、驱动下载链接等。其他配件应提供指引 |
| 69 | ▲管理软件 | 具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能 |
| 70 | ▲增值服务 | ▲厂家升级产品软件与扩容服务 | 提供原厂级的部件/软件产品升级和扩容能力 |
| 71 | ▲提供上门服务 | 具备提供上门服务的能力(可收费) |
| 72 | ▲供应链质量 | ▲抗干扰性 | 当产品部件出现供应风险时，应通知客户并提供风险应对方案确保产品的服务保障，必要时应停止相关受影响产品的销售 |
| 73 | ▲供应能力证明 | 供应商需提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货 |

|  |  |  |
| --- | --- | --- |
| 序号 | 服务 | 参数 |
|  | 部署4节点图片分布式存储，2台光交换机，共提供1.18P的存储空间，支撑非现场违法图片和视频数据的保存 | 1）分布式存储参数：  （数据控制器）内嵌高性能数据存取引擎，用于并行处理所有客户端的数据访问请求，内嵌高性能数据恢复引擎，支持节点间replication（多副本）/N+M（纠删码）数据冗余方式；  \*存储支持SMB/CIFS、NFS、FTP/FTPS、HTTP/HTTPS、POSIX （MPI-IO）S3、.CSI、HDFS、ISCSI、FC、LocalSCSI、Lidrbd、XBD多种访问协议。支持文件、对象及HDFS协议互通，避免因访问协议不同造成的数据拷贝POSIX协议访问延时在10ms以内，支持多套集群挂载和数据一致性。；  \*单目录支持存放大于1000亿文件；单桶支持存放大于1000亿对象；文件系统数量大于4096个，单个文件大小大于256TB；  \*存储支持多租户特性，单个集群内可以划分为多个节点池，不同节点池可设置不同的数据保护策略（动态EC，支持双副本、三副本、4+2、8+2、10+2、12+2、22+2数据保护策略），实现节点池之间数据隔离；对节点池设置不同访问分区，为不同用户或应用提供不同的存储服务，实现数据访问的相互隔离；  \*分布式存储支持分级存储和数据生命周期管理功能。文件接口分级存储和生命周期管理支持文件名过滤规则、文件大小、元数据的创建时间/修改时间；块接口分级存储支持IO监控策略（周期性/定时监控）；桶的生命周期作用于桶内特定对象、桶内所有对象和应用到整个桶，可设置分级存储策略、过期删除策略和过期删除未合并的多段任务策略。分级存储支持四级存储介质，各层级容量均可作为实际容量使用；  \*分布式存储支持目录级的远程复制功能，过滤条件包括文件名、文件大小、文件的访问时间/修改时间/元数据修改时间，支持主从切换、分裂和取消分裂操作以及最大带宽限制；分布式存储支持块接口的远程复制功能，支持可选一致性组复制和LUN复制，支持异步和同步远程复制。分布式存储支持对象接口的远程复制功能，支持桶内所有对象和按照条件筛选（对象名称前缀、对象标签、对象名称前缀及对象标签），支持同步QoS策略（设置传输带宽及TPS上限）以及主从切换；  \*分布式存储系统支持多版本、WORM、对象锁定、追加写、对象加密、重删及压缩、文件迁移至对象特性；  \*分布式存储磁盘或节点故障后，自动触发数据重建修复，1TB数据修复时间小于10分钟；支持调整数据重建QoS策略；  \*分布式存储系统支持文件回收站、块回收站、对象回收站功能，支持文件/对象/存储卷删除后自动保存一段时间，可以从回收站恢复，支持文件过期后自动删除。  \*分布式存储支持原生HDFS接口语义，可对接Hadoop大数据平台并提供存储空间，支持接管Hadoop已有HDFS存储资源。  硬件要求：不低于板载双口千兆RJ45网卡/128G缓存/600G 2.5吋10K 12Gb SAS硬盘\*2 /3.84T 2.5 SATA 6G R SSD\*2 /双口万兆网卡（含模块）\*2 /冗余电源 |
|  | 2）存储硬盘  不低于16TB 3.5吋7.2k 6Gb SATA硬盘\*120 |
|  | 3）光交换机参数：  不低于48个万兆光口（含光模块）+8个100G端口交换机 |

**备注：标\*项参数以第三方检测机构出具的具备CMA标识的检测报告。**

|  |  |  |
| --- | --- | --- |
| 序号 | 服务 | 参数 |
|  | 部署1套国产化数据库支撑业务的正常运转 | 信创国产关系型数据库软件，产品需兼容主流信创CPU芯片和主流信创操作系统。  提供联机交易处理能力，能够通过TPC-C基准测试，测试中3000仓数据量性能达到200万tpmC以上。  数据库在两亿条数据场景下，执行三次前后模糊查询操作，平均查询时间小于0.2毫秒。支持按照全库、用户(模式)和数据表多级的备份和恢复方式。  支持位图索引，索引中存储了表中各列值的位图信息。当列取值少时，位图索引的占用空间要比B树索引更小。  支持RANGE数据类型、表继承、Listen、Notify、混合分区等功能。  为保护业务的连续性，数据库支持高可用集群部署架构，高可用组件，支持双机热备、读写分离、级联复制等数据可靠性的多重保障，对运行态实时保护，健康检查运行监控，一致性校验，控制文件多副本等多重保障；  详细参数见“国产化数据库详细参数要求” |

国产化数据库详细参数如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **一级指标** | **二级指标** | **指标要求** |
| 1 | ▲安装与升级 | ▲数据库安装 | a) 支持命令行或图形化的安装；  b) 支持命令行或图形化的可配置安装能力；  c) 依据安装环境提供相应的初始化参数配置值；  d) 提供图形化软件组件管理向导工具； |
| 2 | ▲数据库重启 | a) 支持命令行或图形化的方式关闭和启动服务；  b) 关闭服务后，再启动服务，服务正常； |
| 3 | ▲安装配置日志 | a) 提供软件安装的日志记录功能；  b) 记录的软件安装信息完整正确；  c) 提供安装配置操作的日志记录功能；  d) 记录的配置操作信息完整正确； |
| 4 | ▲升级维护 | a) 支持版本升级，保证版本间功能和数据的兼容性；  b) 厂商提供当前版本与历史版本的差异说明文档，包含新版本对软件和硬件的支持情况 |
| 5 | ▲数据配置 | ▲参数配置 | a) 依据工作负载和运行环境，提供配置参数修改的能力  b) 修改数据库配置参数后，配置参数立即生效或数据库重新启动生效，立即生效的配置参数和需要数据库重新启动方可生效的配置参数在相关文档中明确； |
| 6 | ▲SQL 功能 | ▲基础数据类型 | a) 支持数值类型；  b) 支持字符类型；  c) 支持二进制类型；  d) 支持日期和时间类型；  e) 支持布尔类型；  f) 支持（大）文本类型；  g) 支持大对象类型 |
| 7 | ▲数据存储基础功能 | 支持基础数据类型 |
| 8 | ▲数据检索基础功能 | 支持基础数据类型 |
| 9 | ▲核心SQL能力 | a) 支持左外连接；  b) 支持右外连接；  c) 支持内连接；  d) 支持全连接 |
| 10 | ▲字符集 | 中文字符集符合 GB 18030 的要求 |
| 11 | ▲常用操作符 | a) 支持逻辑操作符及相关运算；  b) 支持比较操作符及相关运算；  c) 支持算术运算符及相关运算； |
| 12 | ▲条件表达式 | a) 支持对比条件表达式；  b) 支持逻辑条件表达式；  c) 支持空值条件表达式；  d) 支持等于条件表达式；  e) 支持模式匹配条件表达式；  f) 支持区间条件表达式；  g) 支持IN条件表达式；  h) 支持存在条件表达式；  i) 支持以上条件表达式的复合表达式； |
| 13 | ▲SQL执行计划 | 支持SQL计划，使SQL按照指定的语句执行，并实现预期结果 |
| 14 | ▲数据库对象 | ▲基础对象类型 | a) 支持用户的创建、删除、修改；  b) 支持角色的创建、删除、修改；  c) 支持存储过程的创建、删除、修改；  d) 支持表操作功能；  e) 支持自增序列；  f) 支持主键约束、外键约束、唯一性约束、检查约束和联合主键约束；  g) 支持游标功能；  h) 支持视图的创建、删除、修改；  i) 支持数值计算函数、字符处理函数、日期时间值函数、间隔函数、类型转换 函数、位运算函数、聚合函数、格式化、系统信息等常用函数 |
| 15 | ▲基础表分区管理 | a) 哈希分区方式；b) 范围分区方式； c) 列表分区方式 |
| 16 | ▲对象变更 | a)支持数据库的创建、删除、更新以及数据库属性的查询；b)支持在线变更表结构、索引；c)支持数据的增加、删除、修改和查询 |
| 17 | ▲事务能力 | ▲事务基础特性 | 支持事务的ACID |
| 18 | ▲死锁检测与处理 | a) 在并发执行过程中，能检测到死锁；  b) 提供解决全局死锁的机制；  c) 具备死锁处理能力；  d) 具备死锁超时回滚的能力；  e) 具备死锁检测与处理记录功能 |
| 19 | ▲运维 | ▲运行时统计信息基础 功能 | a）数据库慢SQL统计：  1）支持统计 SQL 语句；  2）支持统计用户名；  3）支持统计数据库名；  4）支持统计执行时长；  b）数据库性能状态统计：  1）支持统计每秒事务数和查询数；  2）支持统计 SQL 平均响应时间；  3）支持统计高频 SQL |
| 20 | ▲日志 | a) 具备对各类事件进行日志记录的功能，可通过日志查看操作内容、执行过程和结果；  b) 具备提示和警告功能，提示或警告数据库结构修改、数据库运行配置修改等重要操作；  c) 日志完整正确，并且提供可读文本的形式；  d) 支持中文日志 |
| 21 | ▲远程运维 | 具备远程维护功能 |
| 22 | ▲报警 | a) 厂商提供通知管理员的方法或工具；  b) 支持设置报警基线，数据库运行中遇到重要事件、异常事件和状态、超过报警阈值等情况时，通知管理员；  c) 提供报警API；  d) 报警发生时，支持报警信息的实时展示 |
| 23 | ▲迁移 | ▲数据迁移 | a) 提供元数据、数据库、数据库对象、表数据快速迁移的功能；  b) 支持数据迁移工具实现同构或异构数据库之间的数据迁移；  c) 支持全量数据迁移、增量数据持续同步等迁移模式；  d) 在数据迁移过程中具备应对传输异常的能力，保障数据迁移的稳定性、连续性和一致性；  e) 支持存量数据的一次性迁移和增量数据库的持续同步；  f) 支持多种不同类型的源数据库和目标数据库之间的数据迁移； |
| 24 | ▲数据比对基础功能 | 对源数据库和目标数据库之间的数据进行比对，支持数据一致性，并提供一致性比对报告 |
| 25 | ▲备份恢复 | ▲数据备份 | a) 运行状态下支持对数据库进行全库备份；  b) 运行状态下支持对数据库进行部分备份；  c) 运行状态下支持对数据库进行增量备份； |
| 26 | ▲多种存储媒体备份、 还原 | 支持多种备份存储媒体，支持多种存储 媒体的部分、完整数据库数据还原处理 能力 |
| 27 | ▲备份还原的一致性校 验 | 提供数据库备份数据一致性校验的命令或工具 |
| 28 | ▲集群管理 | ▲集群构建与管理 | a) 支持集群的运行环境；  b) 支持创建并配置数据库集群；  c) 配置信息至少包括日常运维管理、容灾管理、日志管理、备份管理、监控等； |
| 29 | ▲工具 | ▲数据库开发调试工具 | a) 具备图形化功能，提高易用性；  b) 具备导入、编辑、保存、执行 SQL语句和SQL脚本功能；  c) 具备复制、编辑现有数据库对象功能；  d) 具备关键词显示标记、动态语法提示的SQL编辑器功能； |
| 30 | ▲用户、角色管理工具 | 1. 支持创建、修改、删除用户的功能；   b）提供定义用户的功能；  c) 支持创建、修改、删除角色的功能，且提供用户自定义角色的功能； |
| 31 | ▲SQL执行计划查看工具 | a)提供与数据库管理系统进行SQL交互的工具，方便运维工作；  b)支持查看SQL语句查询执行计划与统计信息； |
| 32 | ▲数据库对象工具 | a) 支持创建、修改、删除表的功能，支持定义表结构、约束、存储配置管理的功能；  b) 支持创建、修改、删除索引的功能，支持定义索引结构、类型、存储配置管理的功能；  c) 支持创建、修改、删除视图的功能，支持视图定义的功能；  d) 支持创建、修改、删除约束的功能，支持约束定义的功能 |
| 33 | ▲导入导出工具 | a) 支持导出不同格式，可以将不同格式数据导入到数据库中；  b) 支持不同级别和不同数据库对象的导入/导出功能；  c) 支持从文本文件或者其他上游数据源将数据导入；  d) 支持 SQL 脚本进行导入导出； |
| 34 | ▲数据库运维工具 | a) 支持数据库、数据库存储对象结构、数据、统计信息更新维护；  b) 支持数据库创建、数据库修改、数据库删除、数据库模板维护；  c) 支持数据库任务自动化调度作业管理；  d) 支持图形化展示数据库管理的各种元数据界面，展示的内容具有层次性，包括模式、非模式数据字典信息 |
| 35 | ▲图形化的开发工具 | 厂商提供图形化的开发工具 |
| 36 | ▲图形化运维工具 | 厂商提供图形化的运维工具 |
| 37 | ▲稳定运行 | ▲稳定运行 | a) 支持连续稳定运行；  b) 支持数据库管理系统运行风险的报警能力； |
| 38 | ▲故障切换 | ▲快速切换 | 支持快速切换，在主数据库出现故障时，能够快速切换到备用数据库，保障业务正常运行； |
| 39 | ▲恢复无断点 | 支持无断点恢复能力 |
| 40 | ▲容灾能力 | ▲主备备份 | a) 支持多副本，支持主副本与从副本之间的数据同步，最低时延由生产厂商提供；  b) 提供基于主机的数据库复制技术，包括基于日志的备用数据库远程数据库备份技术，并具备数据副本间的复制  能力； |
| 41 | ▲实例容灾 | a) 在任意数据库实例出现故障时，集群内服务正常运行，数据不丢失，集群整体业务可用；  b) 在实例故障、节点故障等单数据库实例故障时，RPO 时间等于0，RTO时间小于30s |
| 42 | ▲容灾部署 | a)提供远程容灾部署与管理功能；  b)提供生产中心与备份中心之间的容灾部署与管理功能； |
| 43 | ▲同城容灾 | a) 支持同城双中心部署，当主中心故障时，业务切换到备中心；  b) 由于网络、供电等原因造成的可用区级故障，触发集群计划外停机，在同城多可用区场景下，RPO时间等于0，RTO 时间小于1分钟； |
| 44 | ▲容错性 | ▲服务端编程稳定性 | 支持当用户自定义的存储过程、函数运行异常时，数据库稳定运行； |
| 45 | ▲网络容错 | 支持网络中断时，保障事务一致性； |
| 46 | ▲检测报警 | a) 支持数据库实例启动时错误检测能力；  b) 支持加载不同文件格式、不同大小数据出现错误时的故障检测和处理能力；  c) 支持数据库备份执行过程中发生故障时报错或者报警能力；  d) 支持数据库恢复发生故障时报错或者报警能力； |
| 47 | ▲故障恢复 | a) 系统故障重启后能正常运行且支持数据一致性；  b) 支持完全媒体故障恢复的能力；  c) 提供基于时间点故障恢复功能 |
| 48 | ▲不同级别故障可恢复 | 支持数据库事务故障、系统故障、存储 媒体故障不同级别的可恢复能力； |
| 49 | ▲硬件兼容 | ▲硬件平台兼容 | a) 同源支持以下至少三种 CPU 平台架构：  1) ARM；  2) LoongArch；  3) MIPS；  4) SW64；  5) x86；  b) 支持SMP和NUMA的运行环境 |
| 50 | ▲标准兼容 | ▲ODBC | 支持ODBC |
| 51 | ▲JDBC | 支持JDBC |
| 52 | ▲交付方式 | ▲交付方式 | 以光盘、便携式移动设备、镜像文件、在线下载等交付方式提供产品交付物 |
| 53 | ▲服务周期 | ▲产品维护周期 | 产品自发布之日起至产品停止功能升 级（包含不限于新特性、新硬件支持、 问题修复、安全补丁等）之日止≥5 年 |
| 54 | ▲产品延伸服务周期 | 产品停止功能升级之日起至产品停止 功能维护（包括问题修复、安全补丁等） 之日止≥4 年 |
| 55 | ▲产品延伸安全服务周期 | 产品功能维护停止之日起至产品停止 安全维护（包括中高风险漏洞修复）之 日止≥2 年 |
| 56 | ▲售后服务最小保障期 | 服务期内，提供维护； |
| 57 | ▲供应链与服务保障 | ▲供应链与服务保障基础要求 | a) 提供多种形式支持服务，包含电话、电子邮件、远程连接等；  b) 提供技术支持服务，支持同城 4h、异地 12h 响应要求，两个工作日解决问题，对于未能解决的问题和故障提供可行的升级方案；  c) 提供培训材料、产品手册、培训视频等培训相关内容；  d) 建立全国技术服务体系和服务团队，符合专业服务体系标准要求，提供原厂中文服务；  e) 服务周期内支持版本升级；  f) 开源产品对获得的社区源代码进行 安全性和知识产权审查与管理；  g) 提供数据库参数、慢SQL语句的性能优化指南，包含性能优化的具体措施、技巧、案例及建议等 |
| 58 | ▲基本要求 | ▲基本要求 | 数据库应当符合安全可靠测评要求； |
| 59 | ▲基础安全 | ▲漏洞管理 | 建立漏洞管理机制，及时通过邮件、网站等方式将安全漏洞告知用户，并提供 安全补丁对漏洞进行修复 |
| 60 | ▲身份鉴别及访问控制 | 提供身份鉴别及访问控制，加解密的密码要求符合GM/T0028 的相关规定 |

|  |  |  |
| --- | --- | --- |
| 序号 | 服务 | 参数 |
|  | 部署5套国产操作系统支撑业务的正常运转 | 信创国产服务器操作系统，支持龙芯、兆芯、飞腾、鲲鹏、海光、申威等主流国产芯片；  支持以中文引导的图形化界面安装，支持光盘、网络、U盘等多种安装途径安装系统，支持最小化安装；  基础环境：集成Qt等开发框架；  支持 GCC 包含的 C、C++、Objective C、Objective C++ 和 Fortran等相应支持库（libstdc++、libgcj等）；  支持 Python， Perl，Shell，Ruby，PHP 等脚本语言；  支持 java 1.7 、1.8、11 等；  文件系统：默认使用 XFS，支持 EXT3、EXT4、GFS、GFS2 等；  存储支持：内置支持快速块设备作为慢速块设备缓存以加速 IO 支持 swap 压缩以减少 O 并提高性能支持 FCOE、iSCSI，支持将 Ceph 块设备视为常规磁盘设备条目，挂载 到某个目录并使用标准文件系统格式化，比如 XFS 或者 EXT4；  虚拟化支持：支持KVM 虚拟化内置单机虚拟化管理程序支持作为KVM、Xen、Hyper-V、ESXi 虚拟机；  常用应用支持：默认提供 apache http、ftp、DNS、DHCP、MariaDB、PostgreSQL、NFS、 Samba、LDAP 等应用；  含远程服务；5\*8小时电话、邮件等远程支持服务；  详细参数见“国产操作系统单套详细参数要求” |

国产操作系统单套详细参数如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **一级参数指标** | **二级参数指标** | **指标要求** |
| 1 | ▲操作系统支持多CPU架构 | ▲同源兼容多CPU平台架构 | 操作系统支持同源兼容ARM、LoongArch、MIPS、SW64、x86架构的CPU |
| 2 | ▲操作系统支持CPU内置功能 | ▲多核支持 | 操作系统支持双核及多核处理器，包括核间负载均衡、线程绑定等，并提供接口，通过访问接口获取运行状态和控制多核调度 |
| 3 | ▲CPU虚拟化支持 | 操作系统支持CPU虚拟化技术 |
| 4 | ▲动态调节CPU运行频率 | 操作系统根据负载情况，自动调节CPU的运行频率 |
| 5 | ▲支持多CPU | 支持跨路内存访问，支持CPU间负载均衡，支持并优化NUMA体系架构 |
| 6 | ▲支持CPU内置安全功能 | 操作系统支持CPU硬件密码运算与随机数生成等功能；提供编程接口供应用程序调用；支持通过硬件指令判别临界区冲突；支持调用CPU指令，实现自旋锁 |
| 7 | ▲安装部署 | ▲安装方式 | 操作系统支持光盘安装、USB闪存盘安装、网络安装和无人值守安装 |
| 8 | ▲安装模式 | 操作系统支持图形或文本安装模式 |
| 9 | ▲安装过程配置 | 操作系统支持安装界面文种设置、逻辑分区配置（如LVM）、自定义分区设置、安装组件设置、时区设置、键盘布局设置、初始用户设置、计算机名设置和网络设置，支持通过USB闪存盘等方式加载硬件驱动、支持设置加密文件系统 |
| 10 | ▲系统引导 | a)操作系统应支持UEFI2.0及以上规范固件引导，当计算机以UEFI模式启动安装时，安装程序应分配ESP，并在ESP中放置启动引导文件，使系统能以UEFI模式引导；  b)支持bootloader引导，支持MBR及GPT |
| 11 | ▲引导修复 | 操作系统安装媒体提供系统引导修复功能，当已安装的系统引导被破坏时，可重建系统引导 |
| 12 | ▲引导参数编辑 | 操作系统支持用户编辑引导参数，支持GRUB口令保护 |
| 13 | ▲数据保护 | 安装程序在安装执行前明确提示用户可能会删除已有数据，并提供退出/取消功能，当用户取消安装时，不改变硬盘上已有数据 |
| 14 | ▲分辨率自适应 | 操作系统安装完成后应自动适配显示器最佳分辨率(文本模式除外) |
| 15 | ▲安装配置正确性校验 | 操作系统安装和配置过程中，如用户自定义的某些配置可能会影响系统启动或正常使用，予以明确提示 |
| 16 | ▲系统内核 | ▲内核要求 | a)若操作系统是基于Linux内核的服务器操作系统应兼容4.19版内核  b)若操作系统属于其他类型内核不做要求 |
| 17 | ▲进程、线程调度 | ▲NUMA | 操作系统支持基于NUMA的亲和调度 |
| 18 | ▲多核轮询 | 操作系统支持CPU多核轮询调度 |
| 19 | ▲进程调度 | 操作系统具备进程优先级动态调整能力，允许在进程运行时对优先级进行调整；区分实时进程与非实时进程，分别进行调度；支持进程运行状态检查 |
| 20 | ▲内存管理 | ▲内存容量 | 操作系统支持最大内存不小于4TB |
| 21 | ▲内存大页管理 | 操作系统允许应用申请内存大页降低页表转换 |
| 22 | ▲NUMA | 操作系统支持NUMA近节点优化 |
| 23 | ▲存储管理 | ▲RAID支持 | 操作系统支持硬RAID和软RAID，支持软RAID级别0、1、5、6、10 |
| 24 | ▲虚拟文件系统 | 操作系统支持将不同功能的外部设备抽象为统一的文件操作接口，包括存储、输入输出设备 |
| 25 | ▲文件管理 | 操作系统支持文件存储、检索和共享 |
| 26 | ▲可移动存储 | 操作系统支持对可移动外部存储的管理，包括启停、禁用、恢复等 |
| 27 | ▲外部独立存储 | 操作系统支持使用外部独立存储设备 |
| 28 | ▲多路径聚合 | 操作系统支持存储多路径聚合及I/O动态负载均衡 |
| 29 | ▲故障检测 | 操作系统支持硬盘损坏或老化检测及信息收集 |
| 30 | ▲虚拟内存 | 操作系统支持将硬盘的特定分区或文件作为虚拟扩展内存用于存放内存数据，支持虚拟内存压缩 |
| 31 | ▲网络块设备挂载 | 操作系统支持FCoE、iSCSI，支持将Ceph块设备视为常规存储设备挂载到某个目录并作为标准文件系统使用 |
| 32 | ▲网络管理 | ▲网络链路检测 | 操作系统支持网络链路故障检测、链路事件通知和链路状态查询 |
| 33 | ▲TCP卸载引擎 | 操作系统支持运行TCP协议卸载引擎的网卡 |
| 34 | ▲网络协议 | 操作系统支持IPv4、IPv6 |
| 35 | ▲多网卡绑定 | 操作系统支持多网卡绑定 |
| 36 | ▲文件系统 | ▲文件系统支持 | 操作系统支持XFS、EXT3、EXT4、NTFS、FAT32等文件系统，支持相应格式分区创建、删除、格式化等 |
| 37 | ▲日志式文件系统 | 操作系统支持日志式文件系统 |
| 38 | ▲文件处理能力 | 操作系统支持最大文件不小于4TB，最大分区与文件系统不小于10PB，最大文件名长度不小于255字节 |
| 39 | ▲分区大小调整 | 操作系统支持动态调整分区大小，对系统分区容量进行改变 |
| 40 | ▲应用开发运行环境 | ▲集成开发环境/开发框架 | 操作系统通过内置、软件仓库或附加光盘等方式提供开发环境，包括Qt、Eclipse、VSCode等 |
| 41 | ▲开发工具库 | 操作系统通过内置、软件仓库或附加光盘等方式提供开发库，包括GNUC、GNUC++、Java、Qt、Gtk+、Cairo、OpenGL、Perl、Python、Ruby、Rust、Golang、JS等 |
| 42 | ▲编译器开发工具 | 操作系统通过内置、软件仓库或附加光盘等方式提供编译开发工具，包括GCC、G++、Binutils、GDB、Make、CMake等 |
| 43 | ▲文本编辑工具 | 操作系统通过内置、软件仓库或附加光盘等方式提供文本编辑工具，包括Emacs、Vim等 |
| 44 | ▲软件包管理 | 操作系统支持查询软件包描述和包含文件，以及软件包依赖；支持在安装时自动提示并下载安装缺失的依赖软件包 |
| 45 | ▲开发文档 | 供应商应提供软件开发参考文档、驱动开发参考文档、应用移植开发文档、API文档 |
| 46 | ▲服务支持 | ▲网络服务 | 操作系统支持TCP/UDP |
| 47 | ▲网络共享 | 操作系统支持基于NFS、SMB、FTP、CIFS等协议的数据网络共享服务 |
| 48 | ▲WEB服务 | 操作系统支持基于HTTP、HTTPS、FastCGI等协议WEB服务 |
| 49 | ▲加密传输服务 | 操作系统支持基于IPSec和SSL协议的隧道加密传输服务 |
| 50 | ▲数字证书服务 | 操作系统支持基于PKI体系的数字证书服务 |
| 51 | ▲访问控制服务 | 操作系统支持基于RBAC(基于角色的访问控制)机制的访问控制服务 |
| 52 | ▲网络管理服务 | 操作系统支持基于SNMP、NETCONF、RESTCONF等协议的网络管理服务 |
| 53 | ▲时间同步服务 | 操作系统支持基于NTP协议网络时间同步服务 |
| 54 | ▲远程连接服务 | 操作系统支持RPC、rsync、SSH等远程服务 |
| 55 | ▲邮件服务 | 操作系统支持基于SMTP、POP3、IMAP等的邮件服务 |
| 56 | ▲身份鉴别服务 | 操作系统支持基于轻量级目录访问协议的统一身份鉴别服务 |
| 57 | ▲数据存储和查询服务 | 操作系统支持结构化和非结构化格式数据的存储和查询服务 |
| 58 | ▲数据存储和查询服务 | 操作系统支持块、文件、对象等类型的数据存储服务 |
| 59 | ▲数据存储和查询服务 | 操作系统支持SQL、NoSQL、键值等类型的数据库 |
| 60 | ▲存储服务 | 操作系统支持多种传输速率和存储协议的SAN和NAS存储 |
| 61 | ▲集群支持 | 操作系统支持服务基于主备机制的分布式集群、高可用集群的部署模式 |
| 62 | ▲集群支持 | 操作系统支持服务基于分布式通信协议的分布式集群、高可用集群的部署模式 |
| 63 | ▲集群支持 | 操作系统支持基于虚拟路由器冗余协议的高可用集群部署模式 |
| 64 | ▲分布式服务 | 操作系统支持基于同步、异步请求处理机制的分布式服务 |
| 65 | ▲负载均衡模式 | 操作系统支持基于OSI模型的4/7层和链路层的负载均衡模式 |
| 66 | ▲负载均衡模式 | 操作系统支持基于不同调度算法的负载均衡模式 |
| 67 | ▲高可用服务 | 操作系统提供对HA的支持，支持多种集群配置模式，包括主主模式、主备模式、N+1模式和N+M模式，支持资源及节点故障检测 |
| 68 | ▲虚拟化 | ▲虚拟化部署 | 操作系统支持在KVM、Xen、Hyper-V虚拟机上安装部署操作系统 |
| 69 | ▲内核虚拟化(KVM) | 操作系统支持KVM虚拟化：对虚拟机进行启、停等管理操作；对虚拟机硬盘做快照并从快照恢复；兼容qemu、libvirt标准接口；  支持UEFI或legacyBIOS方式启动；  支持虚拟时钟arch-timer；  支持虚拟鼠标、键盘、触控板、声卡、显卡、硬盘、CDROM、串口pty/pipe/file等设备；  支持Virtio协议下的虚拟设备，包括串口、blk驱动硬盘、SCSI驱动硬盘、不同后端控制器类型的Virtio网卡(包括内核态、用户态、qemu)、GPU、vsock设备等；  支持硬盘和网卡选择类型VFIO设备；  支持虚拟机CPU、内存、网卡、硬盘等离线调整；  支持虚拟机网卡、硬盘、USB设备热插拔；  支持PCI/PCIE设备直通；  支持虚拟机热迁移和加密传输；  支持虚拟机远程访问；支持虚拟机CPU和I/O线程绑定 |
| 70 | ▲KVM虚拟机管理 | 操作系统支持虚拟机对主机的访问控制；虚拟机可以拥有独立的物理资源，且各个虚拟机之间严格隔离；支持大页内存运行虚拟机；支持三种CPU型号模拟模式，包括直通、宿主模型、自定义；支持虚拟机资源调配控制，包括Numa、CPU、内存、I/O、网卡；支持CPU拓扑模拟和透传 |
| 71 | ▲容器 | ▲容器虚拟化 | 操作系统支持OCI；支持进程命名空间隔离技术包括不限于mnt、pid、ipc、uts、user、network等；支持在同CPU指令架构下的不同规格硬件上无缝分发，保障运行兼容性；支持沙箱扩展；支持面向容器的独立逻辑文件管理，具备在容器创建时指定专用根文件夹，容器内进程文件访问重定向等功能；支持日志查询功能；支持通过控制终端对容器内主进程的标准输入输出对接交互；支持通过控制终端对容器内新建进程的标准输入输出对接交互；支持容器存储卷管理（新增、删除、卷容量配置、自动回收）、卷共享；支持面向容器的网络设备资源分配和使用；支持CNI；支持容器获取物理节点资源信息 |
| 72 | ▲容器 | ▲容器镜像和存储管理 | 操作系统支持容器镜像导入、导出；支持容器镜像分层保存、导入 |
| 73 | ▲容器 | ▲容器资源隔离和调配 | 操作系统支持容器资源在线调整，包括CPU资源、内存资源、I/O资源等；支持文件配额分配、存储带宽资源使用量监控等机制，实现容器级I/O控制能力；支持面向容器的网络带宽调度策略，实现容器级网络带宽分配、使用量监控等机制；支持面向容器的存储空间使用监控、分配机制；支持容器CPU核独占；支持面向容器的CPU时间片资源按需划分机制；支持面向容器的内存分配和回收机制，实现内存使用量跟踪和管理；支持同一集群在线、离线业务混合部署；支持对容器的编排、负载均衡、调度等能力；支持根据容器在线与离线混合部署状态进行资源优先调度，提高计算机资源利用率 |
| 74 | ▲中文支持 | ▲字符编码集 | 操作系统应符合GB18030的要求 |
| 75 | ▲中文帮助文档 | 操作系统内置中文帮助文档 |
| 76 | ▲系统信息查看工具 | 操作系统支持查看系统版本、内核版本、内存容量、CPU型号等信息 |
| 77 | ▲管理工具 | ▲网络管理工具 | 操作系统支持多网口自动连接、网络地址（常被称为“IP地址”）设置、DNS设置、路由设置；支持多网卡链路聚合，模式类型包括但不仅限于轮询、主备、802.3AD动态链路聚合 |
| 78 | ▲日期和时间管理工具 | 操作系统可设置时间同步服务器地址，支持局域网和广域网的同步设置 |
| 79 | ▲日志服务管理工具 | 操作系统支持收集系统日志 |
| 80 | ▲帐户管理工具 | 操作系统支持帐户添加、删除、属性修改等 |
| 81 | ▲用户操作审计工具 | 操作系统支持用户操作痕迹查询 |
| 82 | ▲存储管理工具 | 操作系统支持EXT、XFS、NTFS、FAT、SWAP等多种格式的分区管理 |
| 83 | ▲SNMP协议工具包 | 操作系统支持SNMP设备和操作信息检索 |
| 84 | ▲文本终端连接工具 | 操作系统支持多终端协同管理 |
| 85 | ▲服务管理工具集 | 操作系统支持服务启动与停止，查看服务状态及日志，查询服务启动顺序及依赖关系 |
| 86 | ▲配置管理工具 | 操作系统提供配置管理工具，可以简化任务配置及服务管理 |
| 87 | ▲监控管理工具 | 操作系统支持监控系统资源使用情况，包含CPU、内存、存储I/O、网络I/O等 |
| 88 | ▲守护进程 | 操作系统支持按需启动守护进程，用户可自定义设定需求守护的进程，如遇异常可重新加载，实现应用持续运行 |
| 89 | ▲基础组件兼容 | ▲版本兼容 | 操作系统基础运行库或开发环境向后（向下）兼容，即系统版本升级后，能兼容上一版本所运行的软件与设备 |
| 90 | ▲兼容周期 | 操作系统主版本兼容维护时间自发布之日起不低于5年，包括但不限于安全修复、功能升级、新硬件支持等 |
| 91 | ▲运行环境 | ▲文件系统层次结构 | 供应商应给出长期兼容支持的文件系统层次结构 |
| 92 | ▲运行库 | 供应商应给出长期兼容支持的运行库 |
| 93 | ▲命令 | 供应商应给出长期兼容支持的常用命令 |
| 94 | ▲软件兼容 | ▲集群软件 | 供应商提供兼容的集群软件清单，且至少兼容一款产品 |
| 95 | ▲虚拟化云平台 | 供应商提供兼容的虚拟化平台软件清单，且至少兼容三款产品 |
| 96 | ▲容器云 | 供应商提供兼容的容器云软件清单，且至少兼容三款产品 |
| 97 | ▲存储软件 | 供应商提供兼容的存储软件清单，且至少兼容一款产品 |
| 98 | ▲数据库管理系统 | 供应商提供兼容的数据库软件清单，且至少兼容三款产品 |
| 99 | ▲中间件 | 供应商提供兼容的中间件软件清单，且至少兼容三款产品 |
| 100 | ▲运维平台 | 供应商提供兼容的运维平台软件清单，且至少兼容一款产品 |
| 101 | ▲备份软件 | 供应商提供兼容的备份恢复软件清单，且至少兼容一款产品 |
| 102 | ▲大数据平台 | 供应商提供兼容的大数据平台软件清单，且至少兼容一款产品 |
| 103 | ▲终端防护及杀毒 | 供应商提供兼容的终端防护及杀毒软件清单，且至少兼容一款产品 |
| 104 | ▲网络防护 | 供应商提供兼容的网络防护软件清单，且至少兼容一款产品 |
| 105 | ▲身份认证 | 供应商提供兼容的身份认证软件清单，且至少兼容一款产品 |
| 106 | ▲服务器整机 | 供应商提供兼容的服务器整机品牌及型号清单，且至少兼容一款产品 |
| 107 | ▲AI服务器 | 供应商提供兼容的AI服务器整机品牌及型号清单，且至少兼容一款产品 |
| 108 | ▲存储 | 供应商提供兼容的存储服务器整机品牌及型号清单，且至少兼容一款产品 |
| 109 | ▲部件兼容 | 供应商提供兼容的系统总线、HBA卡、RAID卡、网卡、光纤卡、AI加速卡、GPU、NPU等品牌及型号清单 |
| 110 | ▲稳定性 | ▲操作系统连续运行168小时 | 操作系统高负载下连续常态运行168小时无故障 |
| 111 | ▲备份还原 | ▲备份还原 | 操作系统提供备份还原功能，支持生成系统状态快照及恢复系统状态 |
| 112 | ▲内存纠错 | ▲内存纠错 | 操作系统支持DDR3、DDR4等内存上的ECC查错、纠错 |
| 113 |  | ▲硬盘热插拔 | 硬件支持时，操作系统支持硬盘热插拔 |
| 114 | ▲维护工具 | ▲远程维护 | 操作系统提供远程控制管理工具，支持RDP、SSH、SPICE、VNC等协议，方便用户进行文本或图形化形式的远程连接及维护 |
| 115 | ▲文件完整检查 | 操作系统提供文件系统检查工具，对文件系统完整性进行检测和修复 |
| 116 | ▲内核分析 | 操作系统提供内核性能分析工具，提供性能分析框架，支持对内核函数层面进行分析；提供内核探测工具，支持对内核及用户态程序动态追踪 |
| 117 | ▲日志管理 | ▲日志记录与存储 | 操作系统支持对安全事件的日志记录，包括帐户增删改、成功登录、失败登录、敏感服务开启关闭、配置修改等，日志信息详实，包括所属用户、访问时间、访问地址等；  支持内核异常日志信息的记录和存储；  支持内核崩溃转储机制，系统崩溃时可收集整个内存信息；  支持配置远程日志功能，可将指定日志内容归档到日志服务器；  支持对日志功能进行访问控制，防止未经授权的访问 |
| 118 | ▲日志处理与分析 | 操作系统提供系统错误问题回溯分析工具，对系统崩溃问题及错误问题进行回溯；支持日志切分、一键收集、转储、同步机制 |
| 119 | ▲脆弱性管理 | ▲脆弱性管理 | 操作系统提供故障管理框架，内置故障分析专家系统，可与外部同类型系统互联；具备故障响应、故障警告功能，提供用户接口，支持故障响应、警告信息分发；支持故障管理守护进程，使用统一的传输信道或机制上报故障信息；具备硬件故障信息捕获、紧急处理功能，包括CPU、内存及PCIe设备等硬件的故障；支持诊断/响应组件动态加载机制；提供或支持第三方远程诊断框架及调测工具集，实现远程诊断及调试断点功能支持物理机、虚拟机中操作系统的故障恢复； |
| 120 | ▲热补丁 | ▲热补丁 | 操作系统支持对内核热补丁进行编号，每个热补丁拥有独立编号；支持增量修复以及回滚机制；提供热补丁合法性和一致性校验功能；提供热补丁管理机制和工具，功能至少覆盖补丁查询、安装、移除；提供热补丁升级和回滚系统日志，便于查询或回溯 |
| 121 | ▲系统升级 | ▲升级内容 | 操作系统支持系统增量升级功能，对系统部件、安全补丁等升级 |
| 122 | ▲升级方式 | 操作系统支持在线升级和离线升级 |
| 123 | ▲数据保护 | 操作系统升级不得修改破坏用户数据 |
| 124 | ▲兼容性 | 操作系统升级不得影响原有软硬件兼容性，如有影响应显式的提示告知用户 |
| 125 | ▲回退 | 操作系统提供升级回退机制，能卸载已升级的软件包，恢复系统原有状态，如升级为不可回退，则系统升级前以显式的提示告知用户 |
| 126 | ▲交付方式 | ▲交付方式 | 供应商提供光盘、USB闪存盘、镜像文件（下载）等交付方式 |
| 127 | ▲服务周期 | ▲产品维护周期 | 服务期内，提供维护； |
| 128 | ▲产品延伸服务周期 | 服务期内，提供维护； |
| 129 | ▲产品延伸安全服务周期 | 服务期内，提供维护； |
| 130 | ▲售后服务最小保障期 | 服务期内，提供维护； |
| 131 | ▲售后服务 | ▲原厂服务 | 服务由操作系统厂商的正式员工提供，不由代理商提供 |
| 132 | ▲服务热线电话 | 操作系统厂商为最终用户提供工作日，每日不少于8h（覆盖一般工作时间，具体时间由企业标准给出）中文技术服务热线 |
| 133 | ▲技术服务标准 | 操作系统厂商提供工作日每日不少于8h技术支持服务 |
| 134 | ▲技术服务时效 | 操作系统厂商满足同城4h、异地12h响要求，两个工作日解决问题，对于未能解决的问题和故障提供可行的升级方案 |
| 135 | ▲技术服务保障 | 发生非人为因素故障，在七日内由操作系统厂商原厂人员对产品进行补充或更换 |
| 136 | ▲现场交付与安装调试 | ▲现场安装调试 | 操作系统厂商提供产品安装与现场调试，并提供安装与调试所需的工具和设备 |
| 137 | ▲配套资料 | 交付产品时操作系统厂商提供配套的技术资料，包括但不限于系统说明文件、用户手册（用户安装、操作、维护、故障排除）等 |
| 138 | ▲系统更换 | ▲系统更换 | 服务期内，操作系统厂商支持版本更换（注：更换后不延长服务期） |
| 139 | ▲厂商能力要求 | ▲服务团队 | 操作系统厂商建立全国技术服务体系和服务团队，为客户提供专业的原厂中文服务 |
| 140 | ▲数据安全保障 | ▲数据收集安全保障 | 除用户授权采集的信息外不采集其他数据，相关信息采集无安全风险，相关数据存储在大陆境内 |
| 141 | ▲数据安全保障 | ▲数据供给安全保障 | 涉及数据下载的线上服务物理服务器不出境，包括代码仓库、系统补丁、安全补丁、服务网站等 |
| 142 | ▲代码无风险 | ▲代码无风险 | 操作系统厂商提供源代码，源代码可供第三方机构审查，开源许可合规，代码知识产权无风险，无恶意安全漏洞或后门，代码可追溯、可重构 |
| 143 | ▲基本要求 | ▲基本要求 | 操作系统应当符合安全可靠测评要求 |
| 144 | ▲密码算法支持 | ▲密码算法实现 | 操作系统支持GM/T0002、GM/T0003和GM/T0004规定的密码算法运算 |
| 145 | ▲随机数生成 | 操作系统随机数质量符合GM/T0005《随机性检测规范》或GB/T32915《信息安全技术二元序列随机性检测方法》 |
| 146 | ▲内置数字证书 | 操作系统内置国家电子认证根CA的根证书 |
| 147 | ▲密码协议实现 | 操作系统支持符合GB/T38636—2020的TLCP |
| 148 | ▲安全管理 | ▲防火墙 | 操作系统提供防火墙配置管理工具，支持基于协议、网络地址、端口的访问控制规则配置，规则修改后立即生效；  支持关闭指定服务和端口，包括但不限于关闭远程访问、共享访问等；  支持防止ARP欺骗攻击 |
| 149 | ▲安全框架 | 操作系统提供统一访问控制安全框架 |
| 150 | ▲身份鉴别 | ▲身份鉴别服务 | 用户标识使用帐户名和帐户ID，在操作系统的整个生存周期内用户标识具有唯一性；  支持用户口令复杂度校验及强口令管理；  支持用户口令有效期配置；支持口令鉴别失败控制；  支持口令加密算法配置，用户口令进行加密后以不可逆的密文形式保存；支持禁止根帐户（root）远程登录设置 |
| 151 | ▲访问控制 | ▲自主访问控制 | 允许客体拥有者以普通帐户决定并控制对客体的访问，并阻止非授权用户对客体的访问；普通用户缺省拥有新建、读写和删除私有目录下文件的权限；支持细粒度的自主访问控制，将访问控制的粒度控制在单个用户，对系统中的每一个客体，实现由客体拥有者以指定用户方式确定其对该客体的访问权限，而其他同组用户或非同组的用户和用户组对该客体的访问权则由客体拥有者授予 |
| 152 | ▲强制访问控制 | 操作系统支持对应用程序的访问控制与资源限制，包括对文件、网络等客体的访问控制；支持应用安装控制、应用执行控制 |
| 153 | ▲安全审计 | 操作系统能对身份鉴别的使用、自主访问控制、标记和强制访问控制策略的修改等生成审计日志；审计记录包括：事件类型、事件发生的日期、触发事件的用户、事件成功或失败等字段；支持审计日志查询和导出功能 |
| 154 | ▲漏洞管理 | ▲漏洞管理 | 操作系统支持漏洞编号，每个漏洞独立编号，可直接使用NVDB、CNVD或CVE编号；  漏洞提醒，发现或获悉漏洞信息时，通过系统推送、电子邮件或官方网站等方式通知用户；漏洞修复，对已发现的安全漏洞通过补丁等方式对系统漏洞进行修复；  漏洞列表，提供每个版本已修复的漏洞列表，提供命令或网页等方式方便用户查询漏洞及其修复情况 |

2.3视频业务安全改造

提供视频业务安全改造服务，满足信创要求，包含软件改造和硬件租赁，投标人应保证在服务期内完成软件改造服务和硬件租赁服务上线。 具体内容如下：

（1）软件改造服务，视频专网视频平台国产化系统改造服务为视频监控客户端软件升级服务，主要对客户端进行国产化芯片、操作系统的适配升级。

（2）硬件租赁服务，主要对视频专网视频平台与国产化PC端的交互信令、码流信令进行适配。租赁设备生产日期要求为2024年1月1日以后生产，项目服务期结束后设备处置权归采购人所有；

具体服务器参数如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 服务 | 参数 |
| 1 | 1台视频融合一体机 | 1） 2U机架式  2） 处理器：≥16核CPU  3） 内存：≥64G内存  4） 硬盘：≥2×2T LFFSATA硬盘  5） 接口：≥2个VGA接口；4个USB 接口；1个RJ-45 管理接口  6） 电源：1+1冗余，双≥550 W电源  详细参数见“服务器一体机详细参数要求” |
| 2 | 1台国产操作系统适配网关一体机 | 1） 2U机架式  2） 处理器：≥16核CPU  3） 内存：≥64G内存  4） 硬盘：≥2×2T LFFSATA硬盘  5） 接口：≥2个VGA接口；4个USB 接口；1个RJ-45 管理接口  6） 电源：1+1冗余，双≥550 W电源  详细参数见“服务器一体机详细参数要求” |

服务器一体机详细参数如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **一级性能参数指标** | **二级性能参数指标** | **指标要求** |
| 1 | ▲CPU规格 | ▲CPU 信息 | （1）配置国产架构处理器，支持超线程技术和睿频技术； |
| （2）单颗CPU物理核心数≥16核、主频≥2.2GHz、末级缓存容量≥32MB、线程数≥32、热设计功耗≥180W、支持内存的最高速率≥2933MHz、通道数≥4、位宽≥64位；  供应商应在投标时给出CPU型号； |
| 2 | ▲主板规格 | ▲主板支持的CPU 和内存情况 | 主板支持CPU ≥2颗，内存数量支持≥ 16个，  供应商应在投标时给出主板支持的CPU型号； |
| 3 | ▲主板内存槽数量 | 主板内存槽数量≥16个 |
| 4 | ▲主板存储接口 | 主板支持SAS/SATA/NVMe SSD存储接口； |
| 5 | ▲PCIe 插槽接口 | 符合 PCIe3.0 或以上的高速串行计  算机扩展总线标准，PCIe 的接口速  率与位宽需保证向下兼容 |
| 6 | ▲主板 PCIe 插槽数量及规格 | PCIe插槽≥5，可通过扩展卡进行插  槽扩展； |
| 7 | ▲内存规格 | ▲内存数量 | 内存数量≥4 |
| 8 | ▲内存规格 | 实配≥16GB DDR4\*4 |
| 9 | ▲内存通道 | 支持≥4个内存接口通道 |
| 10 | ▲存储规格 | ▲硬磁盘实配容量 | 实配≥4T |
| 11 | ▲硬盘实配数量 | 实配≥2块； |
| 12 | ▲硬盘插槽数量及规格 | 支持≥12个热插拔3.5硬盘或2.5硬盘 |
| 13 | ▲网络规格 | ▲网口速率和数量 | ≥8个千兆网口RJ45 |
| 14 | ▲外部接口规格 | ▲显示接口 | 配置≥2个VGA接口 |
| 15 | ▲USB 接口 | 配置≥4个USB3.0接口 |
| 16 | ▲电源规格 | ▲电源模块数量 | ≥2 |
| 17 | ▲电源功率 | ≥550W，电源模块功率应有一定冗余， 满足处理器满载时的需求 |
| 18 | ▲整机规格 | ▲外观和结构 | a)服务器的零部件应紧固无松动，可插拔部件应可靠连接，开关、按钮和其它控制部件应灵活可靠，布局应方便使用； |
| b) 产品表面不应有明显的凹痕、划伤、裂缝、变形和污染等。表面涂层均匀，不应起泡、龟裂、脱落和磨损，金属零部件无锈蚀及其它机械损伤； |
| c) 产品表面说明功能的文字、符号和标志应清晰、端正且牢固； |
| d) 应在服务器的显著位置提供运行状态的指示功能，并在随机文件中明确具体含义； |
| e) 机架、机箱的尺寸应符合通用机柜的安装要求，插入总线插座的电路板接口外形尺寸应符合有关总线标准的规定，将机箱固定在机柜上，机箱底面最大下垂变形不得干涉相邻机体； |
| f) 高密度服务器应给出 CPU 个数与机柜高度； |
| g) 服务器尺寸具体要求在随机文件中明确 |
| 19 | ▲尺寸（高×宽×深） | 供应商应在投标时给出产品尺寸； |
| 20 | ▲环境适应性 | 气候环境适应性应符合 GB/T9813.3 的有关规定，工作温度 10～35℃，贮存运输温度-40～55℃；工作相对湿度 35%～80%，贮存运输相对湿度 20％～93%（40℃）；大气压86～106kPa |
| 21 | ▲机械环境适应性 | 机械环境适应性应符合 GB/T9813.3 的有关规定 |
| 22 | ▲噪声 | 符合 GB/T 9813.3 的有关规定，在产品说明中给出具体测试值塔式服务器噪声在空闲状态下不大于 50dB |
| 23 | 机柜规格 | ▲机柜尺寸 | 供应商在投标时给出长度、高度和深度； |
| 24 | ▲主板 | ▲主板外部接口种类 | 支持 USB、显示、管理等接口 |
| 25 | ▲网络功能 | ▲网络功能 | 支持网络连接、网络访问、数据交换和网络管控功能 |
| 26 | ▲CPU功能 | ▲计算处理 | 支持通用计算及虚拟化功能。处理器需集成整型计算单元、浮点计算单元、内存控制器、I/O 模块等，处理器与存储部件、网络部件、I/O部件等组成计算系统，提供数据处理、网络接入等计算相关功能 |
| 27 | ▲密码算法实现 | CPU 芯片应符合 GM/T 0008 的相关规定，或芯片密码模块应符合 GB/T37092 或 GM/T 0028 的相关规定 |
| 28 | ▲电源功能 | ▲电源热插拔 | 整机电源模块应具备热插拔功能 |
| 29 | ▲电源过流保护 | 支持过流及短路保护的功能 |
| 30 | ▲整机功能 | ▲散热方式 | 支持风冷或液冷等散热方式 |
| 31 | ▲管理系统功能 | ▲BMC 固件基础功能 | 1) 支持 DHCP 设置网络功能；  2)支持静态 IP 设置网络功能；  3)支持设备日志记录，包括但不限于登录日志、操作日志和报警日志等功能；  4)支持日志信息导出和记录删除功能；  5)支持通过管理接口向外输出准确的报警信息功能；  6)设备的 BMC 管理软件应能够按报警的严重程度进行区分；  7)支持 IPMI2.0、SNMP 或 Redfish等接口功能；  8)支持键盘、鼠标和视频的重定向、文本控制台的重定向、远程虚拟媒体、高可靠的硬件监控和管理功能；  9)支持基于网络开启、关闭和重启设备的功能，并查询当前设备开机运行状态；  10)支持故障提示功能，并可通过接口读取服务器故障信息；  11)支持基于网络的固件更新功能，包括 BMC 和 BIOS 等；  12)支持基于网络安装操作系统的功能，并可通过网络控制台访问设备；  13)支持通过本地的硬盘或光驱等存储设备，基于网络完成设备的操作系统安装功能；  14)支持通过浏览器打开管理界面并登录功能；  15)支持设置口令策略功能；  16)支持访问权限设置功能，并通过日志记录访问事件；  17)支持对出厂默认的用户名及口令进行安全保护功能，并提供默认口令修改提示；  18)支持读取设备主板的工作环境温度功能；  19)支持读取服务器 CPU 等核心器件的温度功能；  20)支持通过外部管理工具进行 BMC参数设置的功能，并可基于网络通过外部管理工具对 BMC 进行管理；  21)应支持固件版本查询、固件升级  22)支持基于网络实现开关机和复  位控制的功能；  23)BMC 启动时间应不超过 180s，实现功能包括网络、IPMI、散热、传感器服务可用；  24)支持 BMC 固件设置的恢复出厂功能 |
| 32 | ▲BIOS 固件基础功能 | a）支持查看固件版本、内存信息、主板信息、处理器信息和系统时间信息功能；  b）支持上电初始化界面显示 CPU 信息、内存信息、固件版本和部分快捷键信息功能；  c）支持设置界面中英文显示切换功能；  d）支持查看 PCIe 设备信息，SATA  设备信息功能；  e）支持操作系统安装和引导功能，应并向操作系统提供计算机主板信息和服务接口；  f）支持设置启动顺序，并按照设置的启动顺序启动功能；  g）支持安全启动功能；  h）支持设置口令、修改口令、验证口令功能；  i）支持板载显示控制或独立显卡的显示控制功能；  j）支持 RAID 识别和启动功能；k）支持串口重定向功能；  l）支持固件更新功能；  m）支持 BIOS 固件设置的恢复出厂功能；  n）支持网络引导启用和关闭功能 |
| 33 | ▲远程控制 | 支持远程关机和重新启动功能 |
| 34 | ▲操作系统及驱动功能 | ▲操作系统及驱动的升级 | 支持通过网络、闪存盘对操作系统、驱动进行升级 |
| 35 | ▲操作系统功能 | 支持访问控制、安全审计、网络接入鉴别等功能； |
| 36 | ▲中文信息处理功能 | ▲中文信息处理 | 符合 GB 18030 的有关规定 |
| 37 | ▲关键部件安全要求 | ▲关键部件安全要求 | CPU 和操作系统等关键部件应当符合安全可靠测评要求 |
| 38 | ▲固件安全要求 | ▲故障检测 | 支持故障检测功能，可以检测到具体的 FRU（内存、硬盘等）的故障并发出告警 |
| 39 | ▲系统安全要求 | ▲弱口令字典检查 | 支持弱口令字典检查功能，出现在弱口令字典中的字符串不能被设置为用户口令 |
| 40 | ▲白名单访问控制 | 支持基于时间、IP 或 MAC 白名单访问控制 |
| 41 | ▲二次鉴别 | 支持二次鉴别功能。对于用户配置、权限配置、公钥导入等重要的管理操作，已登录用户应通过二次鉴别后，才能执行操作 |
| 42 | ▲密码证书安全加密存储 | 支持对带外管理系统中的用户口令和证书等敏感信息进行加密存储，禁止使用私有的和业界已知不安全的密码算法 |
| 43 | ▲敏感信息安全加密传输 | 支持使用安全的传输加密协议（如SSH 或 HTTPS 等）传输用户的敏感信息 |
| 44 | ▲信息安全要求 | ▲研发过程安全 | 供应商承诺，生产商已建立从需求、设计、开发、测试、维护端到端的开发流程管理机制，输出和保存开发流程中每个阶段的产品需求清单、设计文档、开发文档、测试记录等材料，保证各个流程可追溯； |
| 45 | ▲物理安全 | ▲物理安全 | 安全要求应符合 GB 4943.1 的规定 |
| 46 | ▲限用物质的限量要求 | ▲限用物质的限量要求 | 限用物质的限量应符合 GB/T 26572的要求 |
| 47 | ▲CPU性能 | ▲CPU 主频 | ≥2.2GHz |
| 48 | ▲单 CPU 核数 | ≥16 |
| 49 | ▲单 CPU 末级缓存容量 | ≥32MB |
| 50 | ▲内存性能 | ▲内存速率 | ≥2933MT/s |
| 51 | ▲电源能耗 | ▲电源能耗 | 符合 GB/T 9813.3 的有关规定 |
| 52 | ▲部件兼容性要求 | ▲内存兼容性 | 适配 3 种及以上厂商的内存产品，且均不低于产品支持的内存规格 |
| 53 | ▲固态存储兼容性 | 适配 3 种或以上厂商的固态存储产品，且均不低于产品支持的固态存储设备规格 |
| 54 | ▲网卡兼容性 | 网卡应适配两种或以上厂商产品 |
| 55 | ▲功能卡兼容性 | 内置或适配符合 PCIe 的功能卡，如：网络功能卡、存储功能卡及图形显示功能卡 |
| 56 | ▲外设兼容性 | ▲外设兼容性 | 兼容多种主流生产商的外部设备，包括显示器、键盘、鼠标、闪存盘、移动硬盘、USB 光驱及 KVM 等，要求使用不同厂商的外部设备时，系统均能正常识别和安装驱动 |
| 57 | ▲软件兼容性 | ▲数据库兼容 | 兼容3个及以上厂商的数据库产品； |
| 58 | ▲中间件兼容 | 兼容3个及以上厂商的中间件产品； |
| 59 | ▲平台软件兼容 | 兼容3个及以上厂商的大数据平台； |
| 60 | ▲整机可靠性要求 | ▲整机可靠性 | m1 值（MTBF 的不可接受值）≥100000h； |
| 61 | ▲风扇可靠性 | 风扇寿命≥ 40000h |
| 62 | ▲部件可靠性 | 支持硬盘、电源、风扇热插拔(内置风扇除外) |
| 63 | ▲包装及运输要求 | ▲标志、包装、运输和贮存 | 符合 GB/T 9813.3 和商品包装政府采购需求标准的相关规定 |
| 64 | ▲服务响应 | ▲服务响应 | a) 提供电话、电子邮件、远程连接等多种形式服务；b) 提供同城 4h、异地 12h 技术响应服务，2 个工作日解决问题，对于未能解决的问题和故障应提供可行的升级方案，并提供周转设备；c) 建立全国技术服务体系和服务团体，符合专业服务体系标准要求，提供原厂中文服务；d) 服务周期内提供产品的维修、换件和升级服务 |
| 65 | ▲培训服务 | 供应商提供培训材料、产品手册、培训视频等培训相关内容 |
| 66 | ▲服务周期 | ▲服务周期 | （1）服务期内，提供服务（含换件和维修）； |
| （2）设备停产后继续提供质量保障服务（含备品备件），服务终止时间与最后一批设备交付时间间隔≥6年； |
| （3）产品停止服务时间应提前1年告知客户； |
| （4）产品发布日期需在随机文件中明确。 |
| （5）产品原厂商需通过Q/ZZLH 1001-2022标准的售后服务体系完善程度卓绝级及以上认证 |
| 67 | ▲服务工具要求 | ▲工具要求 | 提供设置服务器硬件、辅助操作系统安装等功能的辅助工具和管理软件。且随附软件应具有合法授权或版权 |
| 68 | ▲驱动安装升级指引 | 提供出厂安装的配件所需的驱动程序，形式包括但不限于驱动光盘、驱动下载链接等。其他配件应提供指引 |
| 69 | ▲管理软件 | 具备资源管理、系统管理、性能监控、健康监控、基于网络控制、报警设置功能 |
| 70 | ▲增值服务 | ▲厂家升级产品软件与扩容服务 | 提供原厂级的部件/软件产品升级和扩容能力 |
| 71 | ▲提供上门服务 | 供应商具备提供上门服务的能力(可收费) |
| 72 | ▲供应链质量 | ▲抗干扰性 | 当产品部件出现供应风险时，应通知客户并提供风险应对方案确保产品的服务保障，必要时应停止相关受影响产品的销售 |
| 73 | ▲供应能力证明 | 供应商需提供供应链稳定承诺书，确保产品的部件在产品服务周期内稳定供货 |

**（三）货运导航数据及运营保障服务**

1、互联网地图导航基础服务

（1）基于货车长宽高重等整体信息，结合限行政策、限行区内黑白名单等信息，为货车做线路规划；提供每天访问量100w次，并发访问个数100个的能力。

（2）基于货车长宽高重等整体信息，结合限行政策、限行区内黑白名单等信息，为货车做导航，提供显示、播报等sdk能力；提供每天访问量100w次，并发访问个数100个的能力。

（3）基于规划的货车通行证线路信息，将其上传到互联网导航平台云端并做持久化保存；提供每天访问量30w次，并发访问个数50个的能力。

（4）基于互联网导航平台云端增加的线路信息，将其与路网绑定，形成唯一的货车通行证线路；提供每天访问量30w次，并发访问个数50个的能力。

（5）基于关键字信息获取周边的POI信息，供货车导航确定起终点；提供每天访问量50w次，并发访问个数100个的能力。

（6）基于定线导航id获取其线路规划的信息，供定线导航；提供每天访问量50w次，并发访问个数50个的能力。

2、城市货运导航数据运营服务

2.1常态化货运交通组织优化调整服务

（1）限行区域数据调整、制作、数据测试、数据发布服务；

（2）禁行区域数据调整、制作、数据测试、数据发布服务；

（3）黑名单道路调整、数据制作、数据测试、数据发布服务；

（4）避让区域的调整、数据制作、数据测试、数据发布服务；

2.2大型活动、节假日等货运交通组织调整服务。

（1）限行区域数据调整、制作、数据测试、数据发布服务；

（2）禁行区域数据调整、制作、数据测试、数据发布服务；

（3）黑名单道路数据制作、数据测试、数据发布服务；

（4）避让区域的调整、数据制作、数据测试、数据发布服务。

2.3省厅行政审批系统、货车通行证系统数据接口对接、数据运营服务

（1）可申请路线修改接口

（2）可申请路线获取接口

（3）办件接收接口

（4）审批结果接收接口

（5）通行证允许申请车辆接收接口

（6）通行证允许申请车辆修改接口

（7）通行证允许申请车辆获取接口

（8）办件审批进度获取接口

（9）通行证允许申请线路接收接口

（10）通行证允许申请线路修改接口

（11）通行证允许申请线路获取接口

（12）获取/刷新数字证书接口

（13）办件接收接口

（14）办件结果接收接口

（15）可申请路线接收接口

2.4大型活动、节假日等期间省厅行政审批系统、货车通行证系统数据接口对接、数据运营服务。

（1）通行证允许申请车辆接收接口

（2）通行证允许申请车辆修改接口

（3）通行证允许申请车辆获取接口

**（四）安全防控风险预警服务**

通过研判分析近期和历史的高发事故或违法查处数据，为安全防控工作提供行动预警、趋势分析、事故地图等数据分析和应用服务，为安全防控工作提供决策依据、力争精准防控，有效提升安全防控管理效能。 具体内容如下：

1、“波次统一行动”预警

针对全市和辖区高发的事故类型，针对“波次统一行动”，提供包含“预警-派单-落地-反馈”闭环流程的行动管理服务，为“波次统一行动”工作提供精准防控决策依据。

1）预警规则与内容

A.行动模式。按照不同时间维度、强度的区分，提供多种行动模式。

B.预警规则数据分析。根据历史行动数据分析提供预警规则推荐值。

C.预警规则。支持根据历史事故数据统计情况，推出不同区域事故连续高发规则；支持设定专项整治行动预警规则。

D.预警规则调整。事故预警数值、预警事故类型可根据不同区域进行配置。

E.预警内容。包含基于上群事故数据的近期全市某类型事故高发相关信息。

F.预警内容推送。提过消息中间件实现预警内容及时推送。

2）派单

A.预警呈现。根据预警规则和推送设定，在列表中查看预警内容、关联区域。

B.预警确认。可查看预警列表内容，人工确认并做派发。

C.大队查收。被派发大队可在系统界面中收到预警消息，查看派单行动信息。大队可根据实际情况关闭无需处理的预警。

3）落地

A.行动落地。在实施过程中线下收集行动相关的执行结果数据。

B.行动执行反馈。实施行动完成后，在系统中反馈本次实施落地情况。

4）反馈

A.反馈数据汇聚。将行动执行结果数据进行自动汇聚，形成统一的反馈库。

B.战果分析配置。配置战果分析模板，将反馈数据进行人工或自动清理。

C.战果查看。根据战果分析模板，自动生成本次行动及全年的战果分析报告。

2、事故与违法查处趋势分析

通过对事故和违法查处变化趋势的数据分析，通过模型分析同事故/违法关联的潜在因素以及违法查处数据，绘制上述因素的变化趋势折线图。

1）可控违法类型筛选

A.专家经验筛选。根据时空属性分析，结合专家的经验和建议，筛选可防控型事故/违法作为分析对象。

B.数据自动筛选。根据时空属性分析，以及近期违法查处数据进行多因素关联分析结果数据，自动推荐、筛选可防控型事故/违法作为分析对象，作为专家经验筛选的补充。

C.可控违法类型调整。参考近期可控违法类型分析的结果数据，以及专家的经验和建议，可对原有筛选的可防控型事故/违法做调整。

2）事故/违法关联的潜在因素分析

A.数据质量分析。对事故/违法数据的数据质量进行初步分析，形成质量分析报告，进行数据质量的修正。

B.基础信息分析。对上述事故/违法类型的各类潜在因素进行基础信息分析，获取事故/违法的分布规律。

C.多因素关联分析模型。将事故/违法关联潜在因素与违法查处数据进行多因素关联分析，设定关联度阈值，形成两者的关联关系模型。

3）趋势分析

A.趋势分析模型配置。根据模型分析结果数据，配置趋势分析模型，生成事故与违法查处趋势分析专题表。

B.趋势分析查看。可以查看各部门某项违法及事故的日趋势，通过折线图对比找到某项违法查处薄弱的部门。

4）事故与违法查处预演

A.目标设定预演。结合趋势分析专题表，用户可设定未来某个周期事故/违法的目标值，给出查处的数量推荐/预期值。

B.目标达到预演。结合趋势分析专题表，用户可设定未来某个周期查处值，给出事故与违法目标预计达到的值。

C.复盘。根据某个周期完成内目标设定或目标达到的预演信息，针对预演的信息和实际执行的结果数据进行分析，复盘预演效果。

3、亡人事故地图

根据大队提供近3年亡人事故，根据事故数据的类型、区域、时间、经纬度等信息，将亡人事故按照不同年限、不同区域进行图上展示，便于从整体、区域上分析亡人事故。

1）事故经纬度数据治理

将2020年起的亡人事故数据中的经纬度信息进行人工治理。

2）亡人事故地图撒点

适配用户已有GIS地图，将2020年起治理后的亡人事故（包含经纬度）数据在GIS地图撒点、展示。

A. 首屏显示。根据登录的用户信息、默认地图图层信息在首屏展示地图撒点。

B. 事故聚合。根据用户在地图图层上的操作，自动将图层范围内的事故进行聚合、分散。

C. 分类显示。在事故地图上根据固定的分类，支持用户可根据提供的分类信息进行筛选，将筛选结果自动在地图上分类显示。

2）权限控制

A.权限配置。支持通过用户组织架构数，配置不同的权限。

B.权限查看。根据不同权限可查看本级及下级亡人事故地图。

3）标签筛选

A.筛选标签管理。根据亡人事故的标签，可配置不同的标签到筛选界面，满足用户筛选标签变化的需求。

B.标签筛选。可按亡人事故的标签来筛选查看不同类型事故的地图分布情况。

C.数据上色。可根据时间范围，将各年数据在地图上使用不同颜色进行上图，便于直观查看各年的亡人事故变化情况。

4、违法查处数据轻应用

数据轻应用模块部分的主要功能为：自动接入不同业务系统的违法数据，通过可视化数据建模和数据展示功能，配置出符合业务需求的违法明细数据和统计指标查询轻应用，便于用户快速查询不同标签的违法数据，起到为基层民警减负的作用。

1）数据接入：支持对接目标数据源，获取应用所需业务数据，实现数据源共享。

2）违法数据治理：从云上获取各业务系统的违法数据，根据日常违法查处工作关注的信息和标签，将各类违法数据治理成违法主题明细数据表。

3）数据查询：根据不同标签数据作为查询条件，自定义选择次维设置数据统计的维度和指标项，满足民警快速获取日常违法数据分析的数据需求。

4）数据管理：自定义配置和保存违法统计指标规则，自动统计违法考核指标并导出报表。

**二）服务要求**

1、应具有较强的云计算及大数据开发、运维及服务能力，应具备网络安全技术、运维及服务能力；

2、应为本项目投入必要安全硬件专业设备进行服务，以成熟技术进行必要的安全保障；

3、应具备公安数据领域云平台和大数据建设能力、安全保障能力和丰富的项目经验。

**三）服务响应时间**

**▲投标人提供7\*24小时响应服务。接到采购人通知后应于30分钟内响应，2小时内解决问题；如现场驻点人员无法解决需投标人公司提供技术支持的，技术支持人员需3小时内到达现场，48小时内解决问题。**

**四）人员要求**

**1、配备数量**

**按照实际工作需要，配备项目负责人1名，驻点人员不少于11名，不得与其他项目兼任。非驻点服务人员根据采购人实际要求进行安排。承担本项目中的实施、服务、安全保障和技术支持工作。**

**2、人员服务时间**

1）项目负责人服务时间：7\*24小时；

2）驻点人员服务时间：5\*8小时，工作时间9：00-17：30；

3）工作地点：杭州市公安局交通警察支队（杭州市文晖路336号）

**3、人员配备标准**

1）**项目负责人配备标准：年龄55周岁（含）以下，本科及以上学历，具有信息化软硬件运维工作服务经验（投标时提供身份证、学历证书、类似业绩合同或业主证明材料、项目负责人与投标人共同出具的在服务期内为本项目提供服务的承诺函或社保证明）。项目负责人主要负责项目整体实施管理、驻点人员管理，及与采购人的沟通协调等工作。**

**2）驻点人员配备标准：年龄55周岁（含）以下，大专及以上学历，具有信息化软硬件运维工作服务经验（投标时提供身份证、学历证书、类似业绩合同或业主证明材料、驻点人员与投标人共同出具的在服务期内为本项目提供服务的承诺函或社保证明）。驻点人员主要负责项目的具体实施工作，接受采购人统一管理，配合采购人工作。**

**驻点人员分工要求如下：**

（1）专网云平台系统运行及数据治理服务、公安网数据治理服务，驻点人员8人，主要工作：

1）日常维护杭州日常数据服务工作，常态化技术支持，完成数据接入及透出、数据开发和技术支持服务。

2）按要求完成每日平台巡查、数据服务链路维护和数据统计分析工作，检查系统运行情况，每周一上报并出具上周的巡检报告，确保系统的稳定运行，在服务期间驻点人员电话应保持畅通。

3）完善数据上云申请流程，完成公安网数据资源的汇聚整合，实现数据统一汇聚。

4）汇聚的数据进行标准化处理，根据公安大数据处理标准要求对数据进行重新整合。

5）以数据应用为导向，提升数据价值密度。

6）保障上云数据链路，负责维护云上链路新建、维护等。

（2）网络安全服务，驻点人员1人，主要工作：配合采购人开展安全运营管理工作，提供5\*8小时服务，负责公安信息网、视频专网、电子政务外网等相关网络的安全运营管理工作。

1）对系统软硬件设施检查检测，系统参数调整；

2）保障系统的正常运行（包括防火墙设置、杀毒库升级、杀毒服务、系统优化等）；

3）重大活动中的保障工作。

4）服务期内提供《应急响应报告》不少于4份、《渗透测试报告》20份、《重保期间安全日报》至少4份、《网络安全事件应急演练报告》1份、《网络安全事件应急预案》1份、服务期结束后提供《网络安全总结报告》1份

（3）货运导航数据及运营保障服务，驻点人员2人

1）提供常态化货运交通组织优化调整数据服务。

2）提供城市货运导航推广运营服务，包括运输企业、货车驾驶员系统使用、信息咨询服务等。

3）提供大型活动保障服务，在大型活动、会议期间，负责货运交通组织调整数据服务。不限于1、限行区域数据调整、制作、数据测试、数据发布服务；2、禁行区域数据调整、制作、数据测试、数据发布服务；3、黑名单道路调整、数据制作、数据测试、数据发布服务；4、避让区域的调整、数据制作、数据测试、数据发布服务等

4）提供系统开发和对接服务，完成常态化的系统正常运行保障和需求实现，包括省厅行政审批系统、货车通行证系统数据接口对接、数据运维服务。

**4、其他要求：**

1）投标人应派驻固定的驻点人员，合同期内人员不得随意变动，因采购人工作存在即时性和突发性，能够随时响应配合采购人的工作，利于合作的顺利开展；人员如需发生变更，投标人应提前48小时通知采购人，经采购人书面同意后方可更换，更换人员需在24小时内到位，确保任何时间都不得出现人员缺位现象，更换人员素质应不低于投标时的承诺。

2）**对于本项目中提供的软硬件，需根据信创要求，完成信创测评，如因投标人原因未符合要求的，需负责整改到位。**

**3）在本项目合同履行过程中，投标人提供的服务中部分内容（货运导航数据及运营保障服务中的城市货运导航数据运营服务）需要由第三方充分配合，相关费用包含在投标报价内，请在投标时充分考虑，投标人投标时提供承诺函（格式自拟）。若合同履行过程中，未按承诺实施，则处以违约金处罚，违约金金额由投标人自行在承诺函中明确，单次违约金金额不低于5万元且不高于20万元。**

**5.培训要求：**

培训对象：采购人相关处室人员。培训人数根据采购人要求确定（不少于5人）。

培训方式：主要为集中授课和现场操作应用指导培训，提供至少一年一次的培训。

培训地点：培训地点由项目投标人与采购人共同协商确定。

培训内容：培训包括安全体系、视频专网数据体系、公安网数据体系以及应用改造流程普及。

培训师资：由投标人提供1名技术人员或工程师。

**五）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）不得将除非主体、非关键性的工作外的合同内容进行分包或转包。

（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10分钟内向采购人报告。

（5）处理合作事项的信息平台应当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2025年8月1日前向采购人提交一份网络安全报告。

（9）其他应当落实的网络安全责任和义务。

**六）保密条款：**

采购人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； 投标人及工作人员违反保密安全管理要求，构成违法犯罪的，采购人将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。

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，应当交还全部资料和数据。

投标人需与采购人签署保密协议，投标人对在项目实施期间所获得的采购人的情报和资料有保密义务（包括但不限于合同服务期内），泄漏秘密应承担的责任。如有违反，按合同的违约条款向采购人支付违约金，造成采购人损失的应予赔偿，涉嫌犯罪的依法追究刑事责任。

若项目涉及分包的，投标人须按照以上保密要求，与分包供应商签订单位保密协议、个人保密承诺书、开展日常保密教育等措施，确保分包供应商严格落实各项保密规定。

1. **安全事故责任条款：**

因投标人或投标人派遣人员工作过错造成的安全管理事故，投标人负全部责任及相关费用。

（六）拟采购标的的商务要求

1.交付（实施）的时间（期限）：2024年8月1日-2025年7月31日,服务空档期（即2024年8月1日至开始提供服务之前)由原供应商（2023年供应商）按照2024年需求提供服务，期间产生的费用由投标人，按照实际服务时间及2024年合同单价与原供应商按实结算。

2.交付（实施）的地点（范围）：杭州市公安局交通警察支队（杭州市拱墅区文晖路336号）。

3.付款条件（进度和方式）

|  |  |  |
| --- | --- | --- |
| 序号 | 付款比例（%） | 付款方式 |
| 1 | 第一期付款：合同签订后5个工作日内，项目具备实施条件后，采购人支付346.98万元，同时采购人收取履约保证金为合同总价1%。 | 国库转账支付 |
| 2 | 第二期付款：服务至2025年3月31日，无任何服务问题,凭双方签字盖章的验收意见、验收小组签字的验收报告、人员清单、学历证书、身份证、工作服务经验、人员变更申请（如有）、驻点人员每日钉钉考勤签到表、租赁设备清单、产品生产日期凭证、产品合格证、质保承诺书、服务方案、专网云平台监测报告、巡检报告、每月考核材料、数据接入清单、系统渗透测试报告、应急响应报告、重保期间安全日报、网络安全事件应急演练报告、网络安全事件应急预案、网络安全保障方案、网络安全重大事项书面报告（如有）、网络安全风险书面报告（如有）、网络安全总结报告、验收报审表、个人保密承诺、单位保密协议、日常保密教育台账、培训材料、分包协议，最多支付至合同总价的65%（已含采购人向投标人支付的第一期及第二期合同价款） | 国库转账支付 |
| 3 | 第三期付款：服务期结束，无任何服务问题，凭双方签字盖章的验收意见、验收小组签字的验收报告、人员清单、学历证书、身份证、工作服务经验、人员变更申请（如有）、驻点人员每日钉钉考勤签到表、租赁设备清单、产品生产日期凭证、产品合格证、质保承诺书、服务方案、专网云平台监测报告、巡检报告、每月考核材料、数据接入清单、系统渗透测试报告、应急响应报告、重保期间安全日报、网络安全事件应急演练报告、网络安全事件应急预案、网络安全保障方案、网络安全重大事项书面报告（如有）、网络安全风险书面报告（如有）、网络安全总结报告、满足信创要求的检测材料、验收报审表、个人保密承诺、单位保密协议、日常保密教育台账、培训材料、分包协议及公示截图等相关资料，经审计确认后（若有），根据合同单价、服务内容、服务天数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供应商支付的款项总额不超过合同总价。

前述采购人按供应商实际履行情况结算付款的方式不影响采购人向供应商再行收取因供应商未全面按照合同约定履行而产生的违约金。

4.售后服务要求：服务类，无售后服务。

5.其他商务要求（包装和运输、保险等）

1）履约保证金退还：验收合格后，无任何质量问题，采购人于收到投标人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，原额（无息）归还履约保证金。

2）投标报价为综合单价，包含人员工资、加班费、《劳动合同法》规定的各类社保费用、办公费、交通费、食宿费、运行维护、技术支持和税金等为完成本项目各项服务可能发生的全部费用。

3）项目实施过程中如发生变更，应严格办理变更手续，采购人及投标人填写《信息化建设项目变更审批表》，说明变更理由和内容，并随附相关文件和监理公司意见，按采购人内控要求变更管理措施，否则该变更内容在款项结算时，采购人有权不予认可。

（七）采购项目的其他要求

一）履约验收

1.履约验收主体

1）采购单位：杭州市公安局交通警察支队

2）是否选择代理机构：🗹是 🞎否

3）是否邀请本项目的其他供应商： 🞎是 🗹否

4）是否邀请专家： 🗹是 🞎否

5）是否邀请服务对象： 🞎是 🗹否

6）其他：/。

2.履约验收时间：第一次验收时间2025年3月31日后，第二次验收时间2025年7月31日服务结束后。

3.履约验收方式： 🞎简易程序 🗹一般程序

4.履约验收程序： 🞎一次性验收 🞎分段验收 🗹分期验收

5.履约验收

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）规定组织对供应商履约的验收。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，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。

2）本项目为信息化项目，根据采购人内控要求,信息化项目服务期满后,项目单位应向市公安局科信局提交《信息化建设项目验收表》及验收所需相应材料,由市公安局科信局按照市政府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终验。

3）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，经政采云政企区平台相关专业随机抽取专家4名），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，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供应商签字盖章。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。

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》。

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，后续验收费用由供应商支付。

6）验收内容

|  |  |  |
| --- | --- | --- |
| 序号 | 验收内容 | 验收标准 |
| 1 | 质量 | 投标人保证其提供的技术手段安全成熟，硬件、软件均有安全保障。租赁硬件满足采购需求要求。 |
| 2 | 进度 | 项目按合同要求服务时间、应急响应的时间等按响应文件落实到位。 |
| 3 | 网络安全责任和保密 | 制定网络安全保障方案和网络安全事件应急预案，减少网络安全风险等。 |
| 服务人员签订保密协议，安全管理制度完善。未发生重大数据丢失和泄漏问题。对项目人员进行保密教育培训并签订保密承诺书，并在项目验收时作为相关资料，一并提交验收小组审核。 |
| 4 | 服务 | 在服务期间，按公安网数据治理服务、专网云平台系统运行及数据治理服务、安全加固服务及应用迁移改造服务、货运导数据及运营保障、安全防控风险预警服务方案实施专业服务。 |
| 在服务期间，投标人的项目组人员对系统运行情况每天进行巡检，并建立巡检台账。 |
| 5 | 人员管理 | 在服务期间，按合同和投标文件投入相应资质的项目管理和技术人员。按合同和投标文件投入相应资质的项目管理和技术人员。 |
| 6 | 培训 | 按合同要求对采购人系统操作人员、系统管理人员、系统运维人员进行培训，形成相应培训记录。 |
| 7 | 台帐 | 要做好日常的台帐记录，做到记录及时、完整。每周巡检记录、租赁总结报告。 |
| 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。 |

7）验收资料：

验收资料和文件是项目验收的重要依据，投标人从项目实施开始就应完整地积累和保管，验收时在职能部门的指导、配合下按照采购人有关要求编目建档。

1. 采购文件
2. 投标文件
3. 采购合同
4. 人员清单、学历证书、身份证、工作服务经验、人员变更申请（如有）；
5. 驻点人员每日钉钉考勤签到表：需采购人经办人、复核人、投标人签字并盖章
6. 租赁设备清单、产品生产日期凭证、产品合格证、质保承诺书；
7. 服务方案；
8. 专网云平台监测报告、巡检报告；
9. 每月考核材料；
10. 数据接入清单；
11. 验收报审表；
12. 系统渗透测试报告；
13. 应急响应报告；
14. 网络安全事件应急预案；
15. 网络安全事件应急演练报告；
16. 重保期间安全日报；
17. 网络安全保障方案、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）、网络安全总结报告；
18. 满足信创要求的检测材料；
19. 其他相关材料：培训材料、分包协议、单位保密协议、个人保密承诺、日常保密教育台账等。

6.履约验收标准

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。

7.履约验收其他事项:无。

二）考核

采购人负责对本项目的管理指导、验收考核等职责，督促中标人履行合同。采购人委托监理单位对中标人服务工作进行考核，考核结果由采购人经办人、审核人、监理单位、中标人签字盖章。如考核周期内重复出现相同扣分情形，累计计算扣除分值。

本考核以月为考核周期，采用百分制计分方式，采购人根据逐条考核事项及对应扣分对投标人（人员）进行计分。投标人每被扣1分，扣除违约金1000元，违约金在结算合同尾款时扣除。考核分值高于90分（含90分）视为合格，90分以下视为不合格；如投标人经采购人考评连续两次均为不合格，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。如给采购人造成损失的有权向投标人提出索赔。

每月考核表（2024年 月）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 中标单位 | | |  | | |
| 序号 | 考核内容 | | | 考核 扣分 | 备注 |
| 1 | 交通管理数据全生命周期运营服务 | 按采购人实际需求完成当月交通管理数据全生命周期运营服务所要求的内容及数量（不限于采购人电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。 | |  |  |
| 2 | 安全加固及应用迁移改造服务 | 按采购人实际需求完成安全加固及应用迁移改造服务所要求的内容及数量（不限于采购人电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。在服务周期中，如因未按照合同要求进行服务或工作失误，导致发生重大安全事故并被上级部门通报的，每发生一次扣10分。 | |  |  |
| 3 | 货运导航数据及运营保障服务 | 按采购人实际需求完成货运导航数据及运营保障服务所要求的内容及数量（不限于采购人电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。 | |  |  |
| 4 | 安全防控风险预警服务 | 按采购人实际需求完成安全防控风险预警服务所要求的内容及数量（不限于采购人电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。 | |  |  |
| 5 | 租赁设备符合情况 | 未按照要求提供设备的，每发生一次扣10分。 | |  |  |
| 6 | 服务响应时间 | 提供7\*24小时响应服务。接到采购人通知后应于30分钟内响应，2小时内解决问题；如现场驻点人员无法解决需投标人公司提供技术支持的，技术支持人员需3小时内到达现场，48小时内解决问题。不满足要求的，每发生一次扣3分。 | |  |  |
| 7 | 人员要求 | 驻点人员数量不符合采购要求的，每发生一次扣5分。 | |  |  |
| 8 | 驻点人员发生变动时未按采购要求提前通知采购人的，每发生一次扣2分。 | |  |  |
| 9 | 培训要求 | 未按采购人要求进行培训的，每发生一次扣3分。 | |  |  |
| 10 | 网络安全及保密 | 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。 | |  |  |
| 投标人未按保密管理条款规定执行的，每发现一次处违约金10000元，如发生泄密事件，除赔偿采购人损失外，还应承担全部法律责任。 | |  |  |
| 11 | 其他 | 其他服务未满足采购人要求的，每发生一次扣1分。 | |  |  |
| 小计 | | | |  |  |
| 采购人项目经办人（签字）：监理人签字（盖章）：  采购人项目审核人（签字、盖章）：投标人项目负责人（签字、盖章）：  日期：日期： | | | | | |

**第四部分** **评标办法**

**评标办法前附表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 评标标准 | 权重/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 \* |
| 一 | **技术和服务方案78分** | | | |
| 1 | 1、交通管理数据安全生命周期运营服务方案应包括①专网云平台系统运行及数据治理；②公安网数据治理，每项方案详细、合理，满足采购需求的得2分，方案不详细、合理，不符合采购需求的不得分，**最高得4分。**  2、安全加固及应用迁移改造服务方案应包括①网络安全服务；②关键业务安全迁移及改造，每项方案详细、合理，满足采购需求的得2分，方案不详细、合理，不符合采购需求的不得分，**最高得4分。**  3、货运导航数据及运营保障服务方案应包括①互联网地图导航基础服务；②城市货运导航数据运营服务，每项方案详细、合理，满足采购需求的得2分，方案不详细、合理，不符合采购需求的不得分，**最高得4分。**  4、安全防控风险预警服务方案应包括①“波次统一行动”预警；②事故与违法查处趋势分析；③亡人事故地图；④违法查处数据轻应用每项方案详细、合理，满足采购需求的得2分，方案不详细、合理，不符合采购需求的不得分，**最高得8分。** | 20 | 主观分 | （一）服务方案（20分） |
| 2 | 投标人提供的分布式存储、交换机硬件设备与需求的吻合程度：投标产品的基本功能、技术指标与需求的吻合程度和偏差情况，标\*项参数以第三方检测机构出具的具备CMA标识的检测报告等为准（并加盖生产厂家公章），技术指标低于需求技术要求或未提供依据的每一项扣减1分，**本项总计7分，扣完为止。** | 7 | 客观分 | （二）投标人提供产品的性能与需求吻合程度(7分) |
| 3 | 1. 投标人承诺采购需求中部分内容（货运导航数据及运营保障服务中的城市货运导航数据运营服务）满足采购需求的得2分，未承诺或不提供的不得分。 2. 投标人所承诺的合同期内，货运导航数据及运营保障服务中的城市货运导航数据运营服务未按承诺履行的扣款金额情况。单次违约金金额不低于5万元且不高于20万元；   得分计算方式：投标人承诺的有效扣款金额的最高额作为评审基准，其最高额为满分；按［扣款金额得分=（承诺的扣款金额/评审基准）×6］的计算公式计算。四舍五入保留2位小数。 | 8 | 客观分 | （三）投标人提供产品证明材料（8分） |
| 4 | 1、承诺服务期内提供《应急响应报告》不少于4份，满足采购需求的得2分，不满足不得分。  2、承诺服务期内提供《渗透测试报告》不少于20份，满足采购需求的得2分，不满足不得分。  3、承诺服务期内提供《重保期间安全日报》不少于4份，满足采购需求的得2分，不满足不得分。  4、承诺服务期内提供《网络安全事件应急演练报告》不少于1份，满足采购需求的得2分，不满足不得分。  5.承诺服务期内提供《网络安全事件应急预案》不少于1份，满足采购需求的得2分，不满足不得分。  6、承诺服务期结束后提供《网络安全总结报告》1份，满足采购需求的得2分，不满足不得分。  7、承诺对于本项目中提供的软硬件，需根据信创要求，完成信创测评，如因投标人原因未符合要求的，需负责整改到位，满足采购需求的得6分，不满足不得分。 | 18 | 客观分 | （四）服务承诺（18分） |
| 5 | **1、年龄：**  ①.项目负责人满足年龄55周岁（含）以下的，得0.5分，不满足不得分。（提供项目负责人身份证、社保证明）；  ②．驻点人员满足年龄55周岁（含）以下的，每满足1人得0.5分，最多得5.5分，不满足不得分。（提供驻点人员身份证、社保证明）；  **2、学历：**  ①.项目负责人具有本科及以上学历的，得0.5分，不满足不得分。（提供学历证书）；  ②．驻点人员具有大专及以上学历的，每满足一人得0.5分，最多得5.5分，不满足不得分。（提供学历证书）；  **3、类似工作经验：**  ①.项目负责人具有信息化软硬件运维工作服务经验的得1分，不满足不得分。（提供类似业绩合同或业主证明材料）；  ②.驻点人员具有信息化软硬件运维工作服务经验的，每满足一人得1分，最高得11分，不满足不得分。（提供类似业绩合同或业主证明材料）  4、承诺非驻点服务人员根据采购人实际要求进行安排，满足采购需求的得2分，不满足不得分。  5、承诺服务人员的工作时间、工作地点满足，采购需求的得2分，不满足不得分。  6、承诺服务人员的工作内容均能达到采购需求的得2分，不满足不得分。 | 30 | 客观分 | （五）服务人员情况（30分） |
| 6 | 承诺培训服务满足采购需求的得2分，不满足不得分。 | 2 | 客观分 | （六）培训服务（2分） |
| 7 | 投标人承诺网络安全责任满足采购需求的得2分，不满足不得分。 | 2 | 客观分 | （七）网络安全责任（2分） |
| 8 | 投标人承诺保密工作满足采购需求的得2分，不满足不得分。 | 2 | 客观分 | （八）保密服务（2分） |
| 9 | 至投标截止时间前三年以来，供应商承担类似网络数据安全运维或信息化平台或软件集成项目的成功经验情况，结合已完成的项目案例和用户反应情况，供应商同时提供的合同、用户验收报告或业主证明作为证明资料，每个案例（以合同签定时间为准）得0.5分，最高得1分。（1分） | 1 | 客观分 | （九）业绩分（1分） |
| 10 | 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）\*10］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货物或服务项目，以及预留份额政府采购货物或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货物或服务项目，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。 | 10 | 客观分 | （十）报价得分（10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。

**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**

**第一部分 合同书**

项目名称：2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务

甲方：杭州市公安局

乙方：

签订地：杭州市

签订日期： 2024 年月日

2024年月日，杭州市公安局以公开招标对2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务项目进行了采购。经评标委员会评定， （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，经杭州市公安局(以下简称：甲方)和 （中标或者成交标供应商名称） (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：本项目以购买服务方式，提供交通管理数据全生命周期运营服务、安全加固及应用迁移改造服务、货运导航数据及运营保障服务、安全防控风险预警服务，要求提供不少于11人驻点服务；

1.2.2 服务标准：通过本项目实施，提供常态化交通数据运维服务，为甲方正常业务运行提供数据支撑、模型支撑、技术保障支撑，完成甲方数据及应用安全迁移改造，实现数据及应用安全合规；

1.2.3 技术保障：/；

1.2.4 服务人员组成：详见附件一；

1.2.5合同 否 （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，本合同单价（含税）标准为： 合同价格清单：详见附件二 。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总价￥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 是 （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 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 是 （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：***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***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并签字时生效。

**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，分包内容：**安全加固及应用迁移改造服务、城市货运导航数据运营服务，**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** |
| 1.3.2 | 单价合同，本合同单价（含税）标准为： 合同价格清单：详见附件二 。服务工作量的计量方式为：根据合同单价、服务内容、服务天数结算合同价款。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总价￥元（大写：元人民币） |
| 1.4.2 | 乙方缴纳合同总价1%履约保证金，支付方式为：（非现金形式/履约保函形式） |
| 1.5.1 | 合同签订后5个工作日内，项目具备实施条件后，甲方支付合同总价40%，同时甲方收取履约保证金为合同总价1%。 |
| 1.5.2 | / |
| 1.5.3 | / |
| 1.6.2 | 第一期付款：合同签订后5个工作日内，项目具备实施条件后，甲方支付346.98万元，同时甲方收取履约保证金为合同总价1%。  第二期付款：服务至2025年3月31日，无任何服务问题,凭双方签字盖章的验收意见、验收小组签字的验收报告、人员清单、学历证书、身份证、工作服务经验、人员变更申请（如有）、驻点人员每日钉钉考勤签到表、租赁设备清单、产品生产日期凭证、产品合格证、质保承诺书、服务方案、专网云平台监测报告、巡检报告、每月考核材料、数据接入清单、系统渗透测试报告、应急响应报告、重保期间安全日报、网络安全事件应急演练报告、网络安全事件应急预案、网络安全保障方案、网络安全重大事项书面报告（如有）、网络安全风险书面报告（如有）、网络安全总结报告、验收报审表、个人保密承诺、单位保密协议、日常保密教育台账、培训材料、分包协议，最多支付至合同总价的65%（已含甲方向乙方支付的第一期及第二期合同价款）  第三期付款：服务期结束，无任何服务问题，凭双方签字盖章的验收意见、验收小组签字的验收报告、人员清单、学历证书、身份证、工作服务经验、人员变更申请（如有）、驻点人员每日钉钉考勤签到表、租赁设备清单、产品生产日期凭证、产品合格证、质保承诺书、服务方案、专网云平台监测报告、巡检报告、每月考核材料、数据接入清单、系统渗透测试报告、应急响应报告、重保期间安全日报、网络安全事件应急演练报告、网络安全事件应急预案、网络安全保障方案、网络安全重大事项书面报告（如有）、网络安全风险书面报告（如有）、网络安全总结报告、满足信创要求的检测材料、验收报审表、个人保密承诺、单位保密协议、日常保密教育台账、培训材料、分包协议及公示截图等相关资料，经审计确认后（若有），根据合同单价、服务内容、服务天数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。 |
| 1.7.1 | 服务交付（实施）的时间（期限）：12个月（2024年8月1日-2025年7月31日）,服务空档期（即2024年8月1日至开始提供服务之前)由原供应商（2023年供应商）按照2024年需求提供服务，期间产生的费用由乙方，按照实际服务时间及2024年合同单价与原供应商按实结算。 |
| 1.7.2 | 服务交付（实施）的地点（地域范围）：杭州市公安局交通警察支队（杭州市文晖路336号） |
| 1.7.3 | 服务交付（实施）的方式：现场交付 |
| 1.7.4.1 | 交付期限：12个月（2024年8月1日-2025年7月31日） |
| 1.7.4.2 | 交付地点：杭州市公安局交通警察支队（杭州市文晖路336号） |
| 1.7.4.3 | 交付方式：现场交付 |
| 1.8.7 | 1）履约保证金在约定期间内（合同签订之日起至项目通过验收，乙方递交退还履约保证金申请前）不予退还。乙方在前述约定期间届满前能履行完合同约定义务事项的，甲方在前述约定期间届满之日起5个工作日内，按乙方缴纳履约保证金的方式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%；  2）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，书面通知甲方解除合同；  3）除不可抗力外，因甲方原因导致变更、中止或者终止政府采购合同的，甲方应当依照合同约定对乙方受到的损失予以赔偿或者补偿。  乙方的违约责任：  1）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。  2）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服务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；  3）合同实施过程中如发生变更，应严格办理变更手续，甲方及乙方填写《信息化建设项目变更审批表》，说明变更理由和内容，并随附相关文件和监理公司意见，按甲方内控要求变更管理措施，否则该变更内容在款项结算时，甲方有权不予认可。合同实施过程中如发生，未办理变更手续的擅自变更，发现一次乙方应向甲方支付5000元违约金，且甲方有权在要求乙方支付违约金的同时，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。  4）乙方擅自将本合同的全部或部分事务转由第三人承担（经甲方书面同意的分包人除外），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。  5）乙方在服务期内提供的服务未达到合同要求的，甲方将根据考核办法（详见附件三）对乙方处以违约金，直至解除合同；  6）乙方如未履行安全责任提供服务的，导致安全事故责任的，由乙方负责，并赔偿一切损失。  7)乙方未按保密管理条款规定执行的，每发现一次处违约金10000元，如发生泄密事件，除赔偿甲方损失外，还应承担全部法律责任。  8）乙方货运导航数据及运营保障服务中的城市货运导航数据运营服务未按承诺履行，每发现一次处违约金（根据乙方投标时承诺金额填写）元  9）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**人民法院起诉。 |
| 2.3.2 | 合同涉及技术成果的归属和收益的分成办法的：无 |
| 2.5 | 详见1.6.2条款 |
| 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 | 乙方按照合同的约定，服务期结束前根据合同要求完成所有服务，甲方按照第一次验收时间：2025年3月31日后；第二次验收时间：2025年7月31日服务结束后（具体验收时间由甲方最终确定并及时通知乙方）的约定进行定期验收。 |
| 2.15.3 | 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。详见附件五履约验收。 |
| 2.19 | 本合同正本壹式陆份，具有同等法律效力，甲乙双方各执叁份。 |

**一）项目服务内容**

**（一）交通管理数据全生命周期运营服务**

1、专网云平台系统运行及数据治理

（1）数据接入服务

将各类信息化系统的结构化、半结构化、非结构化多种类型数据统一接入和预处理，预计接入30多张相关数据库表，每日接入数据量在5.2亿条左右，每日约100GB。

1）接入杭州市机动车卡口过车数据；

2）接入互联网实时交通数据，包含交通事件、拥堵预警等；

3）根据要完成表单的接入工作，每月底提供数据接入清单。

（2）数据加工治理服务

1）数据探查服务：对接入的杭州市机动车卡口过车、交通工程、互联网实时交通等多种类型数据来源进行打标。通过对来源数据存储位置、提供方式、总量和更新情况、业务含义、字段格式和取值分布、数据结构、数据质量等属性进行多维度探查，完成数据识别工作（例如空值率、值域及分布、命名实体、问题数据等多维度探查识别），为数据定义提供依据。

2）数据读取服务：在完成数据探查及数据定义工作后，将杭州市机动车卡口过车、交通工程、互联网实时交通等源数据与数据定义进行对比核验，确保数据质量和准确性。同时，对各种异构数据进行解密、解压、适配等多个环节操作，并对数据进行字符集转换、半结构化数据转换等其他转换，使数据符合数据处理要求的格式，供下一步处理。

3）数据清洗服务：按照数据清洗标准进行杭州市机动车卡口过车、交通工程、互联网实时交通等100多张书库表数据过滤、去重、格转、校验等数据清洗操作，从而实现数据标准化，包括数据对标、数据去重、数据转换以及数据完整性校验、规范性校验、一致性校验等。

4）数据共享服务：以专网云平台数据资源池为数据底座，通过数据共享打通甲方各部门的数据壁垒，加速数据资源由业务需求驱动和聚集，在业务协同上起到数据融合和共用的作用。为交通局日常业务、市局大数据平台、路网运行等场景提供杭州市机动车卡口过车、交通工程、互联网实时交通等数据支撑。

5）数据传输服务：在数据共享和分发过程中，将涉及到一条或多条链路，数据传输将维护数据传输链路安全畅通，保障数据在传输过程中不错、不重、不丢。

6）模型标准化：使用标准化标签设计模型，包括杭州市机动车卡口过车、交通工程、互联网实时交通等众多的数据统计模型、分析模型、监控模型均具备管理和维护标识，便于模型运行维护过程中的统一化和规范化。

7）任务管理：对数据接入过程进行可视化管理，浏览数据接入任务，修改接入任务配置、实时调配任务的资源，设定任务通知等相关内容，保障接入任务顺畅进行。

8）断点传续保障：通过断点记录、断点标识、断点恢复，保障数据在下载或上传时,将下载或上传任务进行切分,每一个部分采用一个线程进行上传或下载,如果碰到网络故障,保障从已经上传或下载的部分开始继续上传下载未完成的部分，确保数据不重复、不缺失，从而提升数据传输效率、提高数据传输稳定性、减少网络带宽占用。

（3）数据透出服务

数据透出开发：按照业务场景的数据需求，提供对应的数据开发服务，实现数据的共享。完成接口透出的开发，可用于进行路网运行、交通事件、交通需求、交通舆情等决策分析业务。

（4）数据统计服务

1）统计类数据开发服务：满足支队日常统计类业务保障，如拥堵统计、事故统计、警情统计等，并实现数字、excel、word等多样式统计结果呈现。

2）持续提供工程类、秩序类等的数据模型、算子模型开发工作，预计开发模型200个。

（5）运营服务

对开发完成的数据魔方等进行运营保障工作。

监测类数据工作：满足支队日常监测类业务保障，如在途量监测、拥堵指数监测、平均速度监测及某重点路段、重点路口拥堵监测等。同时，结合监测类数据接口开发，为甲方的大脑2.0各应用平台提供监测运营保障，每天巡检，每周出具运行监测报告一份。

（6）专网云平台运行保障

针对专网云平台运行提供驻点服务和应急响应，保障平日系统云资源的规划、开通、监测和运营保障。在重大活动和重大节日期间，提供云平台的应急保障。每天巡检，每天出具城市大脑云平台运行监测报告一份。

2、公安网数据治理

（1）数据上云服务

1）数据源管理：对数据接入的源端和目的端进行基本信息维护，提供对接入组件内数据源统一操作管理的能力，支持根据数据源名称搜索数据源，支持各种异构数据源的新增、编辑、删除等操作。

2）数据探查：以可视化配置的形式提供对数据的探查功能，包括数据接入方式探查、业务探查、字段探查、数据项集探查、问题数据探查等，可用于对来源数据存储位置、提供方式、总量和更新情况、取值分布、数据质量等进行多维度探查，以达到认识数据的目的，预计完成约200张表的数据探查工作，主要包括在专网经过初步治理后的数据、以及市局大数据平台中和甲方业务强相关的部分数据。

3）数据定义：包括数据分级分类定义、数据提取策略定义等步骤。按照部标GA/DSJ 230-2019和GA/DSJ 231-2019规范，定义数据项的字段性质分类和字段敏感度分类；对结构化/半结构化数据提取策略进行定义，实现来源数据资源/数据项到目的数据资源/数据项的提取映射关系，为数据治理提供依据。

4）数据读取：建立跨网络、跨平台的数据安全接入通道，为内部及存在信息共享的部门间数据抽取汇聚提供接口通道，支持多源异构数据的源系统读取数据，包括文件读取、数据库读取及服务接口读取等，预计完成约200张表的数据读取工作，主要包括在专网经过初步治理后的数据、以及市局大数据平台中和甲方业务强相关的部分数据。

（2）数据治理服务

1）数据清洗：按照数据清洗标准进行数据过滤、去重、格转、校验等数据清洗操作，从而实现数据标准化，包括数据对标、数据去重、数据格转、数据校验等，预计完成约200张表的数据清洗工作。

2）数据关联：根据数据定义中的关联规则或算法，将数据和其它知识数据、业务数据等进行关联，并输出关联信息，包括关联回填、关联提取。

3）数据提取：按照数据标准进行字段映射提取和处理函数配置，实现对源数据中各类数据的关键信息提取，预计完成约200张表的数据提取工作。

4）数据分发：通过数据分发，实现对提取、清洗、关联、比对和标识后的数据进行分发处理（如：将结果数据对应分发到原始库、资源库等），预计完成约200张表的数据分发工作。

（3）数据开发服务

1）数据指标服务：包括指标计算、指标推送、指标采集；

2）指标计算：基于客户需求完成指标内容的开发，整体流程包括：指标数据对接、指标详细设计、指标代码实现等，预计完成约50类的指标计算工作。

3）指标推送：基于指标注册的更新频率要求将指标结果推送到指标中心，以可视化配置的形式对指标推送任务进行管理，同时支持以查看日志的形式对历史推送情况进行验证，预计完成约50类的指标推送工作。

4）指标采集：指标推送是从指标中心推送指标结果，而指标采集是从指标中心将指标结果进行采集，采集的范围可以根据甲方的实际使用需求进行申请；将指标结果从指标中心进行采集之后可以用于甲方相关业务系统的应用，预计完成约20类的指标采集工作。

5）数据融合服务：支撑客户特殊的数据使用需求，包括：数据关联、数据融合等，生成特定的结果表数据可以用于后续数据建模、数据查询、数据透出等数据使用需求，方便业务使用的同时也可以在数据安全层面进行把控，预计完成约20项的数据融合工作。

6）计算分析服务：基于特定需求完成计算逻辑设计，针对云上已交付的数据治理成果开展统计分析并产出计算结果，满足客户数据分析需求，预计完成约20项的计算分析工作

7）进行现有200类数据魔方业务模型的梳理工作；在数据域进行200类数据魔方模型的重新设计、重新构建等工作（由于视频专网上的数据魔方模型不能直接迁移到数据域，故需要在数据域中将视频专网的里面的魔方重新在进行搭建并维护；因视频专网和数据中的数据存在一定的差距，且为了提升模型的多用途、计算等能力，故进行重构），涉及到的模型包括每日交通量、道路速度统计查询、高峰延误指数、道路早晚高峰速度模型等；实现重构200类数据魔方模型的测试、运行、优化等工作

8）根据业务发展以及云上数据治理需要，新增50个业务类、服务类等相关模型的设计、开发、测试、运营、优化等工作，涵盖交通卡口流量统计模型、卡口间车流OD统计模型等模型。

（4）数据能力支撑

1）数据资源管理：包括资源市场、资源档案、资源审批；

2）资源市场：按照统一的标准规范对数据资源进行管理，实现数据资源科学、有序、安全使用。

3）资源档案：对数据资源进行档案式管理，使的用户更方便地了解和使用数据资源，简化用户认知数据表的难度，提高数据易用性。

4）资源审批：提供资源审批功能供民警进行合理性验证，同时，以线上资源审批工单的形式进行管理，方便后续进行溯源管理。

预计完成200张表的资源的注册与管理工作。

5）服务资源管理：包括服务市场、服务安全。

6）服务市场：以界面化的形式进行表转服务的注册，已发布的数据服务将展示在服务市场中供业务方申请使用。

7）服务安全：以数据应用的身份对服务接口进行白名单权限认证，支持对服务接口进行调用限额，避免单应用的异常调用影响整体系统。

预计完成30个服务的注册与管理工作。

8）数据推送服务：数据推送服务主要用于支撑甲方内部系统在云上的数据使用需求，包括离线数据推送、实时数据推送；

9）离线数据推送：离线数据推送指的是将上云或治理完成的结果表推送到应用方特定的关系型数据库，预计完成50张表的离线数据推送。

10）实时数据推送：实时数据指的是将实时数据推送到应用方的datahub，用于满足应用方的实时数据使用需求，预计完成30张表的实时数据推送。

11）数据透出服务：数据透出服务用于支撑甲方对外的数据共享需求，主要针对历史共享数据清单的数据链路进行梳理与切换，预计完成50张表的数据透出工作。

12）能力中心对接，包括指标中心对接、IT服务平台对接。

13）指标中心对接：包括指标推送与指标采集：指标推送是将甲方的相关系统、模型的成果转化为指标服务，发布到指标中心；指标采集是将指标中心各个业务系统和大屏已经开发好的指标成果进行采集共享，避免重复开发。

14）IT服务平台对接：对接IT服务平台注册的相关服务接口，通过服务接口可以查询其它部门共享的业务系统数据，满足甲方特定的数据使用需求。

（5）数据预警运营

1）上云任务监控运营：对接入组件的运行状况做一个整体的监控、包括任务监控、事件通知以及节点监控，通过监控中心发现任务或者执行节点的异常信息，及时预警通知运营人员，及时解决，预计需要完成400+个接入任务的运营管理。

2）治理任务监控运营：将当前数据治理组件中的异常预警按照预警时间的倒序来进行展示，提供预警时间、处理状态、预警级别、监控对象、预警类型五种筛选条件来对预警进行分类，方便运营人员快速定位并修复数据治理问题，保障数据稳定性，预计需要完成200+个治理任务的运营管理。

3）针对已经完成的200+数据模型和魔方算子进行维护、升级、运营等工作。

**（二）安全加固及应用迁移改造服务**

1、网络安全服务

针对甲方公安网、车管专网与视频专网的现状，公安网的网络安全性能尚能满足现有业务的安全保障工作。视频专网内仅建设有网络安全网关与大量的边界防护设备，网络内部安全隐患较大，故本期着重针对视频专网进行安全保障服务。

（1）漏洞扫描服务

安全漏洞检测是脆弱性识别的重要手段，能够发现设备和系统中存在的风险点，分析技术措施的有效执行，了解漏洞的危害，通过及时修补完善，避免对信息系统造成严重影响。

采用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，扫描完成后并人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提供准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案，协助甲方进行解决。

（2）数据库审计服务

以安全为核心的审计服务，以全面审计和精确审计为基础，通过全面管理手段贯穿安全事件处理生命周期，致力于全面降低安全风险。通过全面审计，深入了解安全事件的多层次方面，包括对潜在威胁的深入分析和对系统漏洞的详尽检查，确保系统在安全方面的高度韧性。强调精确审计，通过高度精细的审计过程，发现并识别任何异常活动，包括微小的安全漏洞和未经授权的访问，有效地防范潜在风险。全面管理贯穿整个安全事件处理生命周期，建立起强大而可持续的安全框架，包括对安全策略的不断优化和更新，以适应不断演变的威胁环境。这项审计服务不仅仅关注技术层面的保障，更注重整个组织的安全文化建设。通过构建的审计服务，实现了全面降低安全风险的目标，为甲方提供持久而可靠的安全保障。

（3）日志审计服务

通过对网络设备、安全设备、主机和应用系统日志进行全面标准化处理，实现一个高效的安全监控体系。通过及时发现各类安全威胁和异常行为事件，以保障甲方业务的持续、安全运营。通过标准化处理各种日志信息，建立一个有机的关联体系，使得管理人员能够从全局的视角深入了解系统运行状态，确保任何潜在威胁都不会对业务造成中断。

基于国际标准的关联分析引擎服务工具，提供全维度、跨设备、细粒度的关联分析，通过透过事件表象还原事件背后的信息，提供真正可信赖的事件追责依据，为业务运行的深度安全提供坚实支持。实现信息资产的统一管理和监控资产的运行状况，提供集中化的统一管理平台工具。完成所有的日志信息集中收集与处理。

通过对整体安全状况的全面审计，在第一时间发现潜在的问题并采取相应的措施。服务通过标准化处理日志信息，确保系统中的各类信息得到规范、统一的管理。通过关联分析引擎服务工具，深入挖掘事件背后的信息，为管理人员提供更为全面的安全视角。

（4）安全运营服务

提供1名专业安全服务人员配合甲方开展安全运营管理工作，提供5\*8小时服务，负责公安信息网、视频专网、电子政务外网等相关网络的安全运营管理工作。协助开展网络安全主管部门安全检查，协助开展等级保护定级、备案、建设整改、测评和监督检查等。

网络安全技术防护策略持续改进主要针对日常安全监测和安全风险检查的结果进行综合分析研判，识别网络安全威胁和脆弱性，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，并定期开展策略配置备份、系统软件、特征库升级等操作。

定期针对日常安全监测和安全风险检查的结果进行综合分析研判，识别网络安全威胁、脆弱性和不合规配置项，从整体网络安全技术防护策略的角度提出准确、有效的改进措施，协助开展策略配置调优，以持续提升安全运行和防护能力。

（5）应急响应服务

应急响应服务通常包括采取远程、现场等紧急措施和行动，恢复业务到正常服务状态；调查安全事件发生的原因，避免同类安全事件再次发生；在需要司法机关介入时，提供法律认可的数字证据等。

安全专家采取远程、现场等方式应对甲方突发的安全事件和安全问题。专家通过事件分析、原因查找、事件处置、证据保留、及事件溯源等方式，快速解决甲方信息安全事件及问题，恢复业务及系统的安全运行，并确保所有事件应急处置过程得到有效控制和记录。

当需要应急响应协助甲方针对应用系统发生安全事件，并产生重大影响时，提供应急资源支持和应急人员支持，评估影响范围、事件抑制、溯源分析和复盘安全事件，协助开展业务恢复工作，并针对安全事件提供有效的整改意见。每年提供不少于4次应急响应服务。

（6）高级渗透测试服务

渗透测试服务是安全专家通过利用目标应用系统的安全弱点，模拟黑客可能使用的攻击方法和漏洞发现技术，以人工渗透为主，漏洞扫描工具为辅，在保证整个渗透测试过程都在可以控制和调整的范围之内，尽可能的获取目标信息系统的管理权限以及敏感信息的过程。

通过真实模拟黑客使用的工具和分析方法对甲方指定的信息系统进行模拟攻击，结合智能工具扫描结果，由网络安全高级专家进行深入的手工测试和分析，旨在识别工具弱点扫描无法发现的问题。这一过程包括先进的渗透测试工具的运用，模拟各类攻击场景，全面评估系统对于潜在威胁的抵抗能力。手工测试和分析与智能工具扫描相结合，通过深入的测试，发现那些仅依靠工具难以察觉的问题，提高对系统安全性的全面把控。服务注重发现系统中存在的潜在问题，如未经授权的访问、敏感数据的泄漏等，并为每个问题提供详尽的反馈和加固建议，确保信息系统能够在未来面对各类安全挑战时更为坚固和可靠。通过全面的、深度的渗透测试将为甲方信息系统提供实用而有效的安全加固方向，确保其在不断演进的网络威胁环境中保持最佳的安全状态。每年提供不少于20个系统的渗透测试服务。

（7）应急预案服务

为了保障应急响应的服务质量，提供修订、完善应急预案服务。协助建立健全应急响应组织以及预防、预警机制，针对信息系统特点和可能的突发性安全事件拟制规范的应急处理流程，落实物质条件、人力和技术支撑等保障措施，制定出规范、全面、体系化的应急预案。

应急预案的制定和完善将规范应急处理行为，避免应急处理过程中出现混乱、无序状况，减少处理过程中错误的发生，从而避免不必要的损失。

（8）应急演练服务

应急演练服务根据国家、行业等相关规章和标准，结合近年发生的安全事件和面临的安全风险，对甲方的网络安全应急预案进行全面评估与修订。基于符合甲方自身组织架构的网络安全应急预案服务，明确各个部门的责任，准备措施以及应对突发事件的配合机制，提供特定场景的安全演练。

根据甲方需求提供特定场景的演练，可选形式：桌面演练、现场演练。桌面推演服务包括：演练场景分析、演练剧本编写、现场调研、人员组织等。现场演练服务内容包括：现状调研、演练方案编制、演练流程编制、现场演练组织、演练总结等。通过应急演练有效检验并完善应急预案、应急流程，提升甲方人员整体应急能力。

（9）重要时期安全专家保障服务

在重要时期，网络安全保障服务在重大活动的前、中、后阶段发挥着至关重要的作用。服务涵盖活动前的安全自查和运维，活动中的日志分析、安全值守、应急响应等，以及活动后的复盘总结。通过真实模拟黑客攻击手段，结合智能工具扫描和深入的手工测试与分析，专业团队识别工具弱点扫描难以发现的问题。这一全方位的服务体系致力于全面提升活动相关网络的安全性，增强网络的防御能力，以为甲方提供安全、快速、有效的安全服务。早期的安全自查和运维消除潜在隐患，实时的分析和值守保障网络安全，而活动后的复盘总结提供宝贵经验教训，不断优化服务流程。这一综合性的服务策略为重要时期的活动提供了强有力的网络支持，确保其在安全、稳定的网络环境中顺利展开，最大程度地降低潜在风险。每年提供不少于4次保障服务并提供安全日报。

（10）跨网数据请求与响应服务

提供跨网数据请求与响应工具，为系统和用户在异构网络环境下实现了高度灵活而无缝的数据交流能力。通过协议适配，服务克服了不同网络通信障碍，确保数据在不同网络之间的顺畅传输。安全性需得到充分保障，采用先进的加密技术、身份验证和访问控制，有效预防未经授权的访问和数据泄露。服务通过优化性能，包括对数据传输通道的优化、带宽管理和网络流量的控制，确保了高效、快速的数据交换；提供适当的错误处理机制，能够及时检测并解决问题，保障数据交流的连续性和稳定性；通过引入校验和机制，确保在数据传输过程中不会发生数据损坏或篡改。

（11）数据交换边界防护服务

提供数据交换边界防护服务工具，在甲方视频专网与公安网业务进行数据交换过程中，提供数据的机密性、完整性和可用性的服务，保护数据在跨网传输和通信过程中的安全。在网络边界部署边界防护工具，对进行细粒度的访问控制。对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；拥有细粒度为端口级，并根据会话状态信息为数据流提供明确的允许/拒绝访问处理，可将会话处于非活跃一定时间或会话结束后终止网络连接并通过限制网络最大流量数及网络连接数以提升安全等访问控制能力。

（12）违规外联监测服务

引入先进的监测技术和安全审计工具，实时监测网络流量、检测异常访问和识别不寻常的数据传输模式，以主动发现违规外联行为，提高对潜在威胁的感知。建立快速响应机制，一旦检测到异常行为，立即向本级监管方报告，以便迅速采取应对措施，增强监管方对整个网络系统的掌控。完成监测系统的定期检查和更新，修复系统漏洞，升级防护机制，保持系统的健康状态。采用智能化的边界安全防护系统，通过深度学习和行为分析，系统能够学习并识别正常的网络活动模式，实现对异常行为的自动识别和响应。

2、关键业务安全迁移及改造

2.1合成作战应用迁移服务

提供交管专有云平台合成作战应用向警务云迁移改造服务，满足信创要求，包括人车查询、电动车智控、勤务管理、视频巡查、预警中心、警情打标等模块迁移改造。乙方应保证在服务期内完成该项服务。具体内容如下：

（1）人车查询模块。包括机动车信息查询、驾驶人信息查询，具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、整体系统调试及优化。

（2）电动车智控PC端。电动自行车智控闭环应用根据设定的违法查处、撤控规则，并串联移动端查处应用，支撑违法处置高效开展，绩效考核准确快捷。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（3）勤务管理模块。包含巡防区管理、勤务智检、在线警力、勤务排班等功能。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（4）视频巡查PC端。包括视频巡查处置流程及视频巡查驾驶舱展示。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（5）预警中心。应用对接多个第三方平台数据包括过车、违法等数据，直接预警或通过模型和算法产生预警。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、图片链路调整及保存、整体系统调试及优化。

（6）警情打标模块。包括标签设置、标签项自定义、警情打标、查案打标、标签筛选、相关统计、打标导出详情等功能。具体工作包括：迁移表及数据的整理、应用前后端架构分离、应用升级改造、安全访问改造、应用配置改造、应用数据链路调整、整体系统调试及优化。

2.2非现场执法平台升级改造服务

提供支队非现场执法平台软件迁移改造服务，满足信创要求，包括软件服务以及硬件支撑环境搭建服务。乙方应保证在服务期内完成该项服务。具体内容如下：

（1）提供软件服务，包括非现场平台功能迁移、特色需求优化迁移、平台数据对接和扩容、平台业务接口迁移、专网数据转发、非现场功能升级等服务，构建公安网环境下的支队非现场执法平台，支撑非现场业务的高效运转。

1）非现场平台功能迁移服务：主要涉及将现有非现场执法平台的所有功能迁移至新的软件平台。这包括但不限于数据采集、处理、存储、查询和分析等功能的完整迁移。

2）特色需求优化迁移服务：由于业务需求可能存在差异，因此需要进行特定的优化以满足甲方特色需求。包括优驾容错功能的优化、急事通功能的完善等。

3）平台数据对接和扩容服务：在迁移过程中，需要确保新旧平台之间的数据无缝对接，同时考虑到未来数据增长的需求，进行必要的扩容准备，以支撑更大规模的数据处理和分析。

4）平台业务接口迁移服务：对于与外部系统或应用之间的业务接口，需要进行相应的迁移，以确保与外部系统的兼容性和数据交互的顺畅性。

5）专网数据转发服务：在视频和专网采集的非现场数据，统一经过安全边界摆渡至公安网侧。

6）非现场功能升级服务：根据中国信息安全评测中心发布的《安全可靠测评工作指南》要求，需要对非现场执法平台的功能进行升级和改进。涉及到使用国产信创产品来构建新的平台，以满足公安网环境下对数据安全和隐私保护的高标准要求。

（2）支队非现场执法平台硬件支撑环境搭建服务。

2.3视频业务安全改造

提供视频业务安全改造服务，满足信创要求，包含软件改造和硬件租赁，乙方应保证在服务期内完成软件改造服务和硬件租赁服务上线。 具体内容如下：

（1）软件改造服务，视频专网视频平台国产化系统改造服务为视频监控客户端软件升级服务，主要对客户端进行国产化芯片、操作系统的适配升级。

（2）硬件租赁服务，主要对视频专网视频平台与国产化PC端的交互信令、码流信令进行适配。

**（三）货运导航数据及运营保障服务**

1、互联网地图导航基础服务

（1）基于货车长宽高重等整体信息，结合限行政策、限行区内黑白名单等信息，为货车做线路规划；提供每天访问量100w次，并发访问个数100个的能力。

（2）基于货车长宽高重等整体信息，结合限行政策、限行区内黑白名单等信息，为货车做导航，提供显示、播报等sdk能力；提供每天访问量100w次，并发访问个数100个的能力。

（3）基于规划的货车通行证线路信息，将其上传到互联网导航平台云端并做持久化保存；提供每天访问量30w次，并发访问个数50个的能力。

（4）基于互联网导航平台云端增加的线路信息，将其与路网绑定，形成唯一的货车通行证线路；提供每天访问量30w次，并发访问个数50个的能力。

（5）基于关键字信息获取周边的POI信息，供货车导航确定起终点；提供每天访问量50w次，并发访问个数100个的能力。

（6）基于定线导航id获取其线路规划的信息，供定线导航；提供每天访问量50w次，并发访问个数50个的能力。

2、城市货运导航数据运营服务

2.1常态化货运交通组织优化调整服务

（1）限行区域数据调整、制作、数据测试、数据发布服务；

（2）禁行区域数据调整、制作、数据测试、数据发布服务；

（3）黑名单道路调整、数据制作、数据测试、数据发布服务；

（4）避让区域的调整、数据制作、数据测试、数据发布服务；

2.2大型活动、节假日等货运交通组织调整服务。

（1）限行区域数据调整、制作、数据测试、数据发布服务；

（2）禁行区域数据调整、制作、数据测试、数据发布服务；

（3）黑名单道路数据制作、数据测试、数据发布服务；

（4）避让区域的调整、数据制作、数据测试、数据发布服务。

2.3省厅行政审批系统、货车通行证系统数据接口对接、数据运营服务

（1）可申请路线修改接口

（2）可申请路线获取接口

（3）办件接收接口

（4）审批结果接收接口

（5）通行证允许申请车辆接收接口

（6）通行证允许申请车辆修改接口

（7）通行证允许申请车辆获取接口

（8）办件审批进度获取接口

（9）通行证允许申请线路接收接口

（10）通行证允许申请线路修改接口

（11）通行证允许申请线路获取接口

（12）获取/刷新数字证书接口

（13）办件接收接口

（14）办件结果接收接口

（15）可申请路线接收接口

2.4大型活动、节假日等期间省厅行政审批系统、货车通行证系统数据接口对接、数据运营服务。

（1）通行证允许申请车辆接收接口

（2）通行证允许申请车辆修改接口

（3）通行证允许申请车辆获取接口

**（四）安全防控风险预警服务**

通过研判分析近期和历史的高发事故或违法查处数据，为安全防控工作提供行动预警、趋势分析、事故地图等数据分析和应用服务，为安全防控工作提供决策依据、力争精准防控，有效提升安全防控管理效能。 具体内容如下：

1、“波次统一行动”预警

针对全市和辖区高发的事故类型，针对“波次统一行动”，提供包含“预警-派单-落地-反馈”闭环流程的行动管理服务，为“波次统一行动”工作提供精准防控决策依据。

1）预警规则与内容

A.行动模式。按照不同时间维度、强度的区分，提供多种行动模式。

B.预警规则数据分析。根据历史行动数据分析提供预警规则推荐值。

C.预警规则。支持根据历史事故数据统计情况，推出不同区域事故连续高发规则；支持设定专项整治行动预警规则。

D.预警规则调整。事故预警数值、预警事故类型可根据不同区域进行配置。

E.预警内容。包含基于上群事故数据的近期全市某类型事故高发相关信息。

F.预警内容推送。提过消息中间件实现预警内容及时推送。

2）派单

A.预警呈现。根据预警规则和推送设定，在列表中查看预警内容、关联区域。

B.预警确认。可查看预警列表内容，人工确认并做派发。

C.大队查收。被派发大队可在系统界面中收到预警消息，查看派单行动信息。大队可根据实际情况关闭无需处理的预警。

3）落地

A.行动落地。在实施过程中线下收集行动相关的执行结果数据。

B.行动执行反馈。实施行动完成后，在系统中反馈本次实施落地情况。

4）反馈

A.反馈数据汇聚。将行动执行结果数据进行自动汇聚，形成统一的反馈库。

B.战果分析配置。配置战果分析模板，将反馈数据进行人工或自动清理。

C.战果查看。根据战果分析模板，自动生成本次行动及全年的战果分析报告。

2、事故与违法查处趋势分析

通过对事故和违法查处变化趋势的数据分析，通过模型分析同事故/违法关联的潜在因素以及违法查处数据，绘制上述因素的变化趋势折线图。

1）可控违法类型筛选

A.专家经验筛选。根据时空属性分析，结合专家的经验和建议，筛选可防控型事故/违法作为分析对象。

B.数据自动筛选。根据时空属性分析，以及近期违法查处数据进行多因素关联分析结果数据，自动推荐、筛选可防控型事故/违法作为分析对象，作为专家经验筛选的补充。

C.可控违法类型调整。参考近期可控违法类型分析的结果数据，以及专家的经验和建议，可对原有筛选的可防控型事故/违法做调整。

2）事故/违法关联的潜在因素分析

A.数据质量分析。对事故/违法数据的数据质量进行初步分析，形成质量分析报告，进行数据质量的修正。

B.基础信息分析。对上述事故/违法类型的各类潜在因素进行基础信息分析，获取事故/违法的分布规律。

C.多因素关联分析模型。将事故/违法关联潜在因素与违法查处数据进行多因素关联分析，设定关联度阈值，形成两者的关联关系模型。

3）趋势分析

A.趋势分析模型配置。根据模型分析结果数据，配置趋势分析模型，生成事故与违法查处趋势分析专题表。

B.趋势分析查看。可以查看各部门某项违法及事故的日趋势，通过折线图对比找到某项违法查处薄弱的部门。

4）事故与违法查处预演

A.目标设定预演。结合趋势分析专题表，用户可设定未来某个周期事故/违法的目标值，给出查处的数量推荐/预期值。

B.目标达到预演。结合趋势分析专题表，用户可设定未来某个周期查处值，给出事故与违法目标预计达到的值。

C.复盘。根据某个周期完成内目标设定或目标达到的预演信息，针对预演的信息和实际执行的结果数据进行分析，复盘预演效果。

3、亡人事故地图

根据大队提供近3年亡人事故，根据事故数据的类型、区域、时间、经纬度等信息，将亡人事故按照不同年限、不同区域进行图上展示，便于从整体、区域上分析亡人事故。

1）事故经纬度数据治理

将2020年起的亡人事故数据中的经纬度信息进行人工治理。

2）亡人事故地图撒点

适配用户已有GIS地图，将2020年起治理后的亡人事故（包含经纬度）数据在GIS地图撒点、展示。

A. 首屏显示。根据登录的用户信息、默认地图图层信息在首屏展示地图撒点。

B. 事故聚合。根据用户在地图图层上的操作，自动将图层范围内的事故进行聚合、分散。

C. 分类显示。在事故地图上根据固定的分类，支持用户可根据提供的分类信息进行筛选，将筛选结果自动在地图上分类显示。

2）权限控制

A.权限配置。支持通过用户组织架构数，配置不同的权限。

B.权限查看。根据不同权限可查看本级及下级亡人事故地图。

3）标签筛选

A.筛选标签管理。根据亡人事故的标签，可配置不同的标签到筛选界面，满足用户筛选标签变化的需求。

B.标签筛选。可按亡人事故的标签来筛选查看不同类型事故的地图分布情况。

C.数据上色。可根据时间范围，将各年数据在地图上使用不同颜色进行上图，便于直观查看各年的亡人事故变化情况。

4、违法查处数据轻应用

数据轻应用模块部分的主要功能为：自动接入不同业务系统的违法数据，通过可视化数据建模和数据展示功能，配置出符合业务需求的违法明细数据和统计指标查询轻应用，便于用户快速查询不同标签的违法数据，起到为基层民警减负的作用。

1）数据接入：支持对接目标数据源，获取应用所需业务数据，实现数据源共享。

2）违法数据治理：从云上获取各业务系统的违法数据，根据日常违法查处工作关注的信息和标签，将各类违法数据治理成违法主题明细数据表。

3）数据查询：根据不同标签数据作为查询条件，自定义选择次维设置数据统计的维度和指标项，满足民警快速获取日常违法数据分析的数据需求。

4）数据管理：自定义配置和保存违法统计指标规则，自动统计违法考核指标并导出报表。

**二）服务要求**

1、应具有较强的云计算及大数据开发、运维及服务能力，应具备网络安全技术、运维及服务能力；

2、应为本项目投入必要安全硬件专业设备进行服务，以成熟技术进行必要的安全保障；

3、应具备公安数据领域云平台和大数据建设能力、安全保障能力和丰富的项目经验。

**三）服务响应时间**

**乙方提供7\*24小时响应服务。接到甲方通知后应于30分钟内响应，2小时内解决问题；如现场驻点人员无法解决需乙方公司提供技术支持的，技术支持人员需3小时内到达现场，48小时内解决问题。**

**四）人员要求**

**1、配备数量**

**按照实际工作需要，配备项目负责人1名，驻点人员不少于11名，不得与其他项目兼任。非驻点服务人员根据甲方实际要求进行安排。承担本项目中的实施、服务、安全保障和技术支持工作。**

**2、人员服务时间**

1）项目负责人服务时间：7\*24小时；

2）驻点人员服务时间：5\*8小时，工作时间9：00-17：30；

3）工作地点：杭州市公安局交通警察支队（杭州市文晖路336号）

**3、人员配备标准**

1）**项目负责人配备标准：年龄55周岁（含）以下，本科及以上学历，具有信息化软硬件运维工作服务经验（投标时提供身份证、学历证书、类似业绩合同或业主证明材料、项目负责人与乙方共同出具的在服务期内为本项目提供服务的承诺函或社保证明）。项目负责人主要负责项目整体实施管理、驻点人员管理，及与甲方的沟通协调等工作。**

**2）驻点人员配备标准：年龄55周岁（含）以下，大专及以上学历，具有信息化软硬件运维工作服务经验（投标时提供身份证、学历证书、类似业绩合同或业主证明材料、驻点人员与乙方共同出具的在服务期内为本项目提供服务的承诺函或社保证明）。驻点人员主要负责项目的具体实施工作，接受甲方统一管理，配合甲方工作。**

**驻点人员分工要求如下：**

（1）专网云平台系统运行及数据治理服务、公安网数据治理服务，驻点人员8人，主要工作：

1）日常维护杭州日常数据服务工作，常态化技术支持，完成数据接入及透出、数据开发和技术支持服务。

2）按要求完成每日平台巡查、数据服务链路维护和数据统计分析工作，检查系统运行情况，每周一上报并出具上周的巡检报告，确保系统的稳定运行，在服务期间驻点人员电话应保持畅通。

3）完善数据上云申请流程，完成公安网数据资源的汇聚整合，实现数据统一汇聚。

4）汇聚的数据进行标准化处理，根据公安大数据处理标准要求对数据进行重新整合。

5）以数据应用为导向，提升数据价值密度。

6）保障上云数据链路，负责维护云上链路新建、维护等。

（2）网络安全服务，驻点人员1人，主要工作：配合甲方开展安全运营管理工作，提供5\*8小时服务，负责公安信息网、视频专网、电子政务外网等相关网络的安全运营管理工作。

1）对系统软硬件设施检查检测，系统参数调整；

2）保障系统的正常运行（包括防火墙设置、杀毒库升级、杀毒服务、系统优化等）；

3）重大活动中的保障工作。

4）服务期内提供《应急响应报告》不少于4份、《渗透测试报告》20份、《重保期间安全日报》至少4份、《网络安全事件应急演练报告》1份、《网络安全事件应急预案》1份、服务期结束后提供《网络安全总结报告》1份

（3）货运导航数据及运营保障服务，驻点人员2人

1）提供常态化货运交通组织优化调整数据服务。

2）提供城市货运导航推广运营服务，包括运输企业、货车驾驶员系统使用、信息咨询服务等。

3）提供大型活动保障服务，在大型活动、会议期间，负责货运交通组织调整数据服务。不限于1、限行区域数据调整、制作、数据测试、数据发布服务；2、禁行区域数据调整、制作、数据测试、数据发布服务；3、黑名单道路调整、数据制作、数据测试、数据发布服务；4、避让区域的调整、数据制作、数据测试、数据发布服务等

4）提供系统开发和对接服务，完成常态化的系统正常运行保障和需求实现，包括省厅行政审批系统、货车通行证系统数据接口对接、数据运维服务。

**4、其他要求：**

1）乙方应派驻固定的驻点人员，合同期内人员不得随意变动，因甲方工作存在即时性和突发性，能够随时响应配合甲方的工作，利于合作的顺利开展；人员如需发生变更，乙方应提前48小时通知甲方，经甲方书面同意后方可更换，更换人员需在24小时内到位，确保任何时间都不得出现人员缺位现象，更换人员素质应不低于合同要求。

2）对于本项目中提供的软硬件，需根据信创要求，完成信创测评，如因乙方人原因未符合要求的，需负责整改到位。

**3）在本项目合同履行过程中，乙方提供的服务中部分内容（货运导航数据及运营保障服务中的城市货运导航数据运营服务）需要由第三方充分配合，相关费用包含在合同总价内，乙方提供承诺函（格式自拟）。若合同履行过程中，未按承诺实施，则处以违约金处罚，违约金金额由乙方自行在承诺函中明确，单次违约金金额不低于5万元且不高于20万元。**

**5.培训要求：**

培训对象：甲方相关处室人员。培训人数根据甲方要求确定（不少于5人）。

培训方式：主要为集中授课和现场操作应用指导培训，提供至少一年一次的培训。

培训地点：培训地点由项目乙方与甲方共同协商确定。

培训内容：培训包括安全体系、视频专网数据体系、公安网数据体系以及应用改造流程普及。

培训师资：由乙方提供1名技术人员或工程师。

**五）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）不得将除非主体、非关键性的工作外的合同内容进行分包或转包。

（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10分钟内向甲方报告。

（5）处理合作事项的信息平台应当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2025年8月1日前向甲方提交一份网络安全报告。

（9）其他应当落实的网络安全责任和义务。

**六）保密条款：**

甲方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； 乙方及工作人员违反保密安全管理要求，构成违法犯罪的，甲方将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。

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，应当交还全部资料和数据。

乙方需与甲方签署保密协议，乙方对在项目实施期间所获得的甲方的情报和资料有保密义务（包括但不限于合同服务期内），泄漏秘密应承担的责任。如有违反，按合同的违约条款向甲方支付违约金，造成甲方损失的应予赔偿，涉嫌犯罪的依法追究刑事责任。

若项目涉及分包的，乙方须按照以上保密要求，与分包供应商签订单位保密协议、个人保密承诺书、开展日常保密教育等措施，确保分包供应商严格落实各项保密规定。

**七）安全事故责任条款：**

因乙方或乙方派遣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。

**八）履约验收：**

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，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。

2）本项目为信息化项目，根据甲方内控要求,信息化项目服务期满后,项目单位应向市公安局科信局提交《信息化建设项目验收表》及验收所需相应材料,由市公安局科信局按照市政府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终验。

3）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，经政采云政企区平台相关专业随机抽取专家4名），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。

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

|  |  |  |
| --- | --- | --- |
| 序号 | 验收内容 | 验收标准 |
| 1 | 质量 | 乙方保证其提供的技术手段安全成熟，硬件、软件均有安全保障。租赁硬件满足采购需求要求。 |
| 2 | 进度 | 项目按合同要求服务时间、应急响应的时间等按响应文件落实到位。 |
| 3 | 网络安全责任和保密 | 制定网络安全保障方案和网络安全事件应急预案，减少网络安全风险等。 |
| 服务人员签订保密协议，安全管理制度完善。未发生重大数据丢失和泄漏问题。对项目人员进行保密教育培训并签订保密承诺书，并在项目验收时作为相关资料，一并提交验收小组审核。 |
| 4 | 服务 | 在服务期间，按公安网数据治理服务、专网云平台系统运行及数据治理服务、安全加固服务及应用迁移改造服务、货运导数据及运营保障、安全防控风险预警服务方案实施专业服务。 |
| 在服务期间，乙方的项目组人员对系统运行情况每天进行巡检，并建立巡检台账。 |
| 5 | 人员管理 | 在服务期间，按合同和投标文件投入相应资质的项目管理和技术人员。按合同和投标文件投入相应资质的项目管理和技术人员。 |
| 6 | 培训 | 按合同要求对甲方系统操作人员、系统管理人员、系统运维人员进行培训，形成相应培训记录。 |
| 7 | 台帐 | 要做好日常的台帐记录，做到记录及时、完整。每周巡检记录、租赁总结报告。 |
| 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。 |

7）验收资料：

验收资料和文件是项目验收的重要依据，乙方从项目实施开始就应完整地积累和保管，验收时在职能部门的指导、配合下按照甲方有关要求编目建档。

1. 采购文件
2. 投标文件
3. 采购合同
4. 人员清单、学历证书、身份证、工作服务经验、人员变更申请（如有）；
5. 驻点人员每日钉钉考勤签到表：需甲方经办人、复核人、乙方签字并盖章
6. 租赁设备清单、产品生产日期凭证、产品合格证、质保承诺书；
7. 服务方案；
8. 专网云平台监测报告、巡检报告；
9. 每月考核材料；
10. 数据接入清单；
11. 验收报审表；
12. 系统渗透测试报告；
13. 应急响应报告；
14. 网络安全事件应急预案；
15. 网络安全事件应急演练报告；
16. 重保期间安全日报；
17. 网络安全保障方案、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）、网络安全总结报告；
18. 满足信创要求的检测材料；
19. 其他相关材料：培训材料、分包协议、单位保密协议、个人保密承诺、日常保密教育台账等。

**附件一：项目小组人员表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 姓名 | 身份证号码 | 联系方式 | 本项目承担的职责 | 备注 |
| 1 |  |  |  | 项目负责人 |  |
| 2 |  |  |  | 驻点人员 |  |
| 3 |  |  |  | 驻点人员 |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| … |  |  |  |  |  |

**附件二：合同价格清单**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | 服务模块 | | 服务内容 | 品牌/型号（如有） | 服务要求 | 服务期 | 单价（万元/月） | 合计 （万元） | 备注 |
| 交通管理数据全生命周期运营服务 | 专网云平台系统运行及数据治理 | | 数据接入 |  | 【服务形式】驻点服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 数据加工治理 |  |  |
| 数据透出 |  |  |
| 数据统计 |  |  |
| 运营服务 |  |  |
| 专网云平台运行保障 |  |  |
| 公安网交警数据服务 | | 数据上云服务 |  | 【服务形式】驻点服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 数据治理服务 |  |  |
| 数据开发服务 |  |  |
| 数据能力支撑 |  |  |
| 数据预警运营 |  |  |
| 安全加固及应用迁移改造服务 | 网络安全服务 | | 漏洞扫描服务 |  | 【服务形式】一年提供4次漏洞扫描服务； | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 数据库审计服务 |  | 【服务形式】一次性提供； |  |
| 日志审计服务 |  | 【服务形式】一次性提供； |  |
| 安全运营服务 |  | 【服务形式】驻点服务1人 |  |
| 应急响应服务 |  | 【服务形式】一年提供4次应急响应服务 |  |
| 高级渗透测试服务 |  | 【服务形式】一年提供20个系统的渗透测试服务； |  |
| 应急预案服务 |  | 【服务形式】一年提供一次应急预案服务； |  |
| 应急演练服务 |  | 【服务形式】一年提供一次应急演练服务； |  |
| 重要时期安全专家保障服务 |  | 【服务形式】一年提供4次重要时期安全专家保障服务； |  |
| 跨网数据请求与响应服务 |  | 【服务形式】工具租用，符合信创要求，租赁期满后设备处置权归属甲方所有 |  |
| 数据交换边界防护服务 |  | 【服务形式】工具租用，符合信创要求，租赁期满后设备处置权归属甲方所有 |  |
| 违规外联监测服务 |  | 【服务形式】租赁期内7\*24小时服务 |  |
| 关键业务安全迁移及改造 | | 合成作战应用迁移服务 |  | 【服务形式】一次性提供 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 非现场执法平台升级改造服务 |  | 【服务形式】平台升级改造服务一次性提供；工具租用，符合信创要求，租赁期满后设备处置权归属乙方所有 |  |
| 视频业务安全改造 |  | 【服务形式】视频业务安全改造服务一次性提供；工具租用，符合信创要求，租赁期满后设备处置权归属甲方所有 |  |
| 货运导航数据及运营保障服务 | 互联网地图导航基础服务 | | 货车线路规划 |  | 【服务形式】租赁期内7\*24小时服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 货车导航接口 |  |  |
| 创建路线及绑定-路线增加 |  |  |
| 创建路线及绑定-路线和线路绑定 |  |  |
| 搜索服务-关键字搜索 |  |  |
| 定线导航信息获取服务 |  |  |
|  | 城市货运导航数据运营服务 | | 常态化货运交通组织优化调整数据服务 |  | 【服务形式】驻点服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 大型活动、会议货运交通组织调整数据服务 |  |  |
| 浙江省公安厅行政审批系统、货车通行证系统数据接口对接、数据运营服务 |  |  |
| 大型活动期间浙江省公安厅行政审批系统、货车通行证系统数据接口对接、数据运营服务 |  |  |
| 安全防控风险预警服务 | 安全防控风险预警服务 | | “波次统一行动”预警服务 |  | 【服务形式】工具租用，租赁期满后设备处置权归属甲方所有 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 事故与违法查处趋势分析服务 |  |  |
| 亡人事故地图服务 |  |  |
| 违法查处数据模型服务 |  |  |
|  | | 服务期：2024年8月1日至2025年7月31日。  合同总价（小写）人民币万元  合同总价（大写）人民币万元 | | | | | | |  |

**附件三：考核办法**

甲方负责对本项目的管理指导、验收考核等职责，督促乙方履行合同。甲方委托监理单位对乙方服务工作进行考核，考核结果由甲方经办人、审核人、监理单位、乙方签字盖章。如考核周期内重复出现相同扣分情形，累计计算扣除分值。

本考核以月为考核周期，采用百分制计分方式，甲方根据逐条考核事项及对应扣分对乙方（人员）进行计分。乙方每被扣1分，扣除违约金1000元，违约金在结算合同尾款时扣除。考核分值高于90分（含90分）视为合格，90分以下视为不合格；如乙方经甲方考评连续两次均为不合格，甲方有权无条件终止合同,并没收乙方全部履约保证金。如给甲方造成损失的有权向乙方提出索赔。

每月考核表（2024年 月）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 中标单位 | | |  | | |
| 序号 | 考核内容 | | | 考核 扣分 | 备注 |
| 1 | 交通管理数据全生命周期运营服务 | 按甲方实际需求完成当月交通管理数据全生命周期运营服务所要求的内容及数量（不限于甲方电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。 | |  |  |
| 2 | 安全加固及应用迁移改造服务 | 按甲方实际需求完成安全加固及应用迁移改造服务所要求的内容及数量（不限于甲方电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。在服务周期中，如因未按照合同要求进行服务或工作失误，导致发生重大安全事故并被上级部门通报的，每发生一次扣10分。 | |  |  |
| 3 | 货运导航数据及运营保障服务 | 按甲方实际需求完成货运导航数据及运营保障服务所要求的内容及数量（不限于甲方电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。 | |  |  |
| 4 | 安全防控风险预警服务 | 按甲方实际需求完成安全防控风险预警服务所要求的内容及数量（不限于甲方电话、微信、钉钉、短信等交办的），服务未达到当月要求的，每发生一次扣10分。 | |  |  |
| 5 | 租赁设备符合情况 | 未按照要求提供设备的，每发生一次扣10分。 | |  |  |
| 6 | 服务响应时间 | 提供7\*24小时响应服务。接到甲方通知后应于30分钟内响应，2小时内解决问题；如现场驻点人员无法解决需乙方公司提供技术支持的，技术支持人员需3小时内到达现场，48小时内解决问题。不满足要求的，每发生一次扣3分。 | |  |  |
| 7 | 人员要求 | 驻点人员数量不符合采购要求的，每发生一次扣5分。 | |  |  |
| 8 | 驻点人员发生变动时未按采购要求提前通知甲方的，每发生一次扣2分。 | |  |  |
| 9 | 培训要求 | 未按甲方要求进行培训的，每发生一次扣3分。 | |  |  |
| 10 | 网络安全及保密 | 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。 | |  |  |
| 乙方未按保密管理条款规定执行的，每发现一次处违约金10000元，如发生泄密事件，除赔偿甲方损失外，还应承担全部法律责任。 | |  |  |
| 11 | 其他 | 其他服务未满足甲方要求的，每发生一次扣1分。 | |  |  |
| 小计 | | | |  |  |
| 甲方项目经办人（签字）： 监理人签字（盖章）：  甲方项目审核人（签字、盖章）： 乙方项目负责人（签字、盖章）：  日期：日期： | | | | | |

**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**

杭州市公安局交通警察支队、浙江信达咨询监理有限公司：

我方参与2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：HZSGAJ-2024-17（代)】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**

杭州市公安局交通警察支队、浙江信达咨询监理有限公司：

我方参加你方组织的2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：HZSGAJ-2024-17（代)】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 90 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）**

杭州市公安局交通警察支队、浙江信达咨询监理有限公司：

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2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：HZSGAJ-2024-17（代)】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）**

杭州市公安局交通警察支队、浙江信达咨询监理有限公司：

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2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：

HZSGAJ-2024-17（代)】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**

杭州市公安局交通警察支队、浙江信达咨询监理有限公司：

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）

杭州市公安局交通警察支队、浙江信达咨询监理有限公司：

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2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：HZSGAJ-2024-17（代)】的实施。

**开标一览表（报价表）(单位均为人民币元)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | 服务模块 | 服务内容 | 品牌/型号（如有） | 服务要求 | 服务期 | 单价（万元/月） | 合计 （万元） | 备注 |
| 交通管理数据全生命周期运  营服务 | 专网云平台系统运行及数据治理 | 数据接入 |  | 【服务形式】驻点服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 数据加工治理 |  |  |
| 数据透出 |  |  |
| 数据统计 |  |  |
| 运营服务 |  |  |
| 专网云平台运行保障 |  |  |
| 公安网交警数据服务 | 数据上云服务 |  | 【服务形式】驻点服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 数据治理服务 |  |  |
| 数据开发服务 |  |  |
| 数据能力支撑 |  |  |
| 数据预警运营 |  |  |
| 安全加固及应用迁移改造服务 | 网络安全服务 | 漏洞扫描服务 |  | 【服务形式】一年提供4次漏洞扫描服务； | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 数据库审计服务 |  | 【服务形式】一次性提供； |  |
| 日志审计服务 |  | 【服务形式】一次性提供； |  |
| 安全运营服务 |  | 【服务形式】驻点服务1人 |  |
| 应急响应服务 |  | 【服务形式】一年提供4次应急响应服务 |  |
| 高级渗透测试服务 |  | 【服务形式】一年提供20个系统的渗透测试服务； |  |
| 应急预案服务 |  | 【服务形式】一年提供一次应急预案服务； |  |
| 应急演练服务 |  | 【服务形式】一年提供一次应急演练服务； |  |
| 重要时期安全专家保障服务 |  | 【服务形式】一年提供4次重要时期安全专家保障服务； |  |
| 跨网数据请求与响应服务 |  | 【服务形式】工具租用，符合信创要求，租赁期满后设备处置权归属采购人所有 |  |
| 数据交换边界防护服务 |  | 【服务形式】工具租用，符合信创要求，租赁期满后设备处置权归属采购人所有 |  |
| 违规外联监测服务 |  | 【服务形式】租赁期内7\*24小时服务 |  |
| 关键业务安全迁移及改造 | 合成作战应用迁移服务 |  | 【服务形式】一次性提供 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 非现场执法平台升级改造服务 |  | 【服务形式】平台升级改造服务一次性提供；工具租用，符合信创要求，租赁期满后设备处置权归属投标人所有 |  |
| 视频业务安全改造 |  | 【服务形式】视频业务安全改造服务一次性提供；工具租用，符合信创要求，租赁期满后设备处置权归属采购人所有 |  |
| 货运导航数据及运营保障服务 | 互联网地图导航基础服务 | 货车线路规划 |  | 【服务形式】租赁期内7\*24小时服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 货车导航接口 |  |  |
| 创建路线及绑定-路线增加 |  |  |
| 创建路线及绑定-路线和线路绑定 |  |  |
| 搜索服务-关键字搜索 |  |  |
| 定线导航信息获取服务 |  |  |
| 城市货运导航数据运营服务 | 常态化货运交通组织优化调整数据服务 |  | 【服务形式】驻点服务 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 大型活动、会议货运交通组织调整数据服务 |  |  |
| 浙江省公安厅行政审批系统、货车通行证系统数据接口对接、数据运营服务 |  |  |
| 大型活动期间浙江省公安厅行政审批系统、货车通行证系统数据接口对接、数据运营服务 |  |  |
| 安全防控风险预警服务 | 安全防控风险预警服务 | “波次统一行动”预警服务 |  | 【服务形式】  工具租用，租赁期满后设备处置权归属采购人所有 | 12个月（2024.8.1-2025.7.31） |  |  |  |
| 事故与违法查处趋势分析服务 |  |  |
| 亡人事故地图服务 |  |  |
| 违法查处数据模型服务 |  |  |
|  | 服务期：2024年8月1日至2025年7月31日。  合同总价（小写）人民币万元  合同总价（大写）人民币万元 | | | | | | |  |

**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。

1. 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\_杭州市公安局交通警察支队\_单位的\_2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务\_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**

杭州市公安局交通警察支队、浙江信达咨询监理有限公司：

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2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：HZSGAJ-2024-17（代)】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

2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：HZSGAJ-2024-17（代)】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2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务【招标编号：HZSGAJ-2024-17（代)】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 杭州市公安局交通警察支队的 2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务采购活动，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：

1.2024年杭州交警业务系统使用服务-2024年杭州交警网络及数据安全运维服务，属于 软件和信息技术服务 ；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。