**外高桥保税区域行政通道智能视觉系统招标需求**

一、说明

**1 总则**

1.1 投标人应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由投标人自行负责。

1.2 投标人对所提供的系统应当享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

1.3 投标人提供的货物应当是全新的、未使用过的，货物和相关服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

1.4 投标人应如实准确地填写投标货物的规格型号、技术参数、品牌、产地等相关信息，因上述信息内容填写不完整、不准确，而导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

★1.5若本项目涉及国家强制认证产品（信息安全产品、3C认证产品、强制节能产品、电信设备进网许可证等），则根据国家有关规定，投标人提供的产品必须满足强制认证要求。（详见第一章投标人须知及前附表21.3（9））

★1.6投标人提供的产品和服务必须符合国家强制性标准。

1.7采购人在技术需求和图纸或图片（如果有）中指出的工艺、材料和货物的标准以及参照的技术参数或型号仅起说明作用，并没有任何限制性和排他性，投标人在投标中可以选用其他替代标准、技术参数或型号，但这些替代要在不影响功能实现的前提下，并在可接受范围内接受偏离。

1.8投标人在投标前应认真了解采购人的使用需求、使用条件（使用空间、能源条件等）和其他相关条件，一旦中标，应按照招标文件和合同规定的要求提供货物及相关服务。

1.9投标人应根据本章节中详细技术规格要求，采用市场主流产品或按照要求提供定制产品参加竞标。同时，**请投标人务必注意：无论是正偏离还是负偏离，都不得与招标要求相差太大，否则将可能影响投标人的得分**。一旦中标，投标人应按投标文件的承诺签订合同并提供相应的产品和服务。

1.10本项目如涉及软件开发，则开发软件（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）的全部知识产权归采购人所有。投标人向采购人交付使用的软件系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。支撑该系统开发和运行的第三方编制的软件的知识产权仍属于第三方。如采购人使用该软件系统构成上述侵权的，则由投标人承担全部责任。

1.11投标人认为招标文件（包括招标补充文件）存在排他性或歧视性条款，自收到招标文件之日或者招标文件公告期限届满之日起10日内，以书面形式提出，并附相关证据。

二、项目概况

**2项目名称：外高桥保税区域行政通道智能视觉系统**

**3项目地点：上海市浦东新区基隆路9号**

**4 招标范围与内容**

4.1 项目背景及现状

随着全球经济数字化转型加速和我国对外开放战略的深入推进，外高桥保税区作为上海自贸试验区核心功能区，承载着国际贸易、物流分拨、高端制造等多元化功能，已成为长三角地区外向型经济的重要枢纽。然而，在区域快速发展的背景下，传统管理模式面临多重挑战，亟须亟需通过智能化升级实现治理能力现代化。

外高桥保税区域行政通道智能视觉系统项目的建设背景主要源于以下几个方面的需求现状:

4.1.1 应对保税区发展带来的管理挑战:

外高桥保税区作为上海自贸试验区的核心区域，经济发展蓬勃，外来人口众多，行政通道密布，车流量巨大。然而，传统的人工管理模式效率低下，难以满足日益增长的管理需求，更无法有效应对安全风险防控的挑战。

为解决当前行政通道监管依赖人工、视频覆盖不全、数据维度不完整等问题，保障区域安全稳定，建设外高桥保税区域行政通道智能视觉系统迫在眉睫。

4.1.2 响应国家数字化转型战略:

国家高度重视数字化转型，提出了建设数字中国的战略目标。外高桥保税区作为上海自贸试验区的重要组成部分，需要积极响应国家战略，推动数字化转型，提升区域治理能力。

4.1.3 满足保税区管理与发展需求:

建设一套完善的管理系统，提升保税区人员、车辆出入管理和治安管理效率。

提升安全保障能力，及时发现和处理异常事件，有效预防和减少安全事故的发生。

提高车辆监管效率，实现对进出车辆的实时监控和监管，规范车辆通行秩序。

推动区域数字经济发展，为保税区的数字化治理和经济治理提供有力支持。

4.1.4 契合国家战略与政策要求:

响应《海关总署公告2025年第19号》关于区域管理政策的要求。

响应自贸试验区升级要求，实现特殊监管区域智能监管全覆盖。

响应新基建战略部署，建设“数字孪生口岸”，构建物联感知体系。

落实海关特殊监管区域的安全防控需求，提升区域管理水平。

4.2 项目招标范围及内容

根据上海城市数字化转型的总体战略，聚焦于外高桥保税区域行政通道智能化管理的迫切需求，我们致力于构建外高桥保税区域行政通道智能视觉系统，该系统旨在深度融合人工智能、物联网、大数据等前沿技术，以创新驱动发展，全面提升保税区行政通道的智能化管理水平，有力促进保税区行政通道的智能化、精细化管理，为保税区的安全、高效运营奠定坚实基础。遵循“全面规划、分步实施、高效协同”的原则，本系统旨在实现以下核心建设内容：

4.2.1 智能视觉监控全覆盖

在外高桥保税区域的15个关键出入口，本项目计划部署先进的智能视觉设备，以实现视频监控的全方位、无死角覆盖。这一举措旨在确保行政通道的安全监管无遗漏，为保税区的安全运营提供坚实的保障。通过高清摄像头和智能监控技术的结合，系统能够实时捕捉并记录各出入口的动态情况，有效防范和应对潜在的安全风险。此外，该系统还将支持多画面切换与缩放功能，使监控人员能够清晰地观察到各区域的动态，进一步提升安全监管的效率和准确性。

4.2.2 重点车辆智能监管

利用CMOS智能相机，对进出保税区的车辆进行实时抓拍、车牌识别和车型分类，支持多种车型和车牌类型识别（支持识别大货车、中货车、小货车、大客车、中客车、轿车、面包车、suv、二轮车9种车型，而车牌识别则包括蓝牌、黄牌、绿牌、黄绿牌、黑牌、白牌等多种车牌类型）。系统能够精确提取车辆信息，智能预警异常行驶路径，有效监控违规进出行政通道的货运车辆，提升安全监管的精准性和时效性，为应急指挥和调度提供支持。

4.2.3 数据储存汇总

项目将建立一个集中的数据存储系统，用于汇总和管理车辆视频记录与事件信息。该系统确保所有数据的安全存储，并支持实时检索和历史数据的追溯查询，以便于在需要时快速调取相关信息，进行事件分析和决策支持。

4.2.4 数据互联互通

对接海关跨境贸易大数据平台，实时车辆风险数据共享和业务协同，提升区域治理水平。通过标准化的数据交互接口，实现数据共享的便捷化与高效化，进一步增强不同部门间的业务联动能力。此外，还将提供必要的数据传输安全保障措施和技术支持服务，以保证跨平台的数据安全及稳定运行。

4.3本项目交付日期：自合同签订之日起4个月内。

**5 承包方式**

5.1 依据本项目的招标范围和内容，中标人以包系统设计、包供货、包安装集成调试、包质量、包安全的方式实施总承包。

5.2本项目不允许分包。

**6 合同的签订**

6.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与招标文件和中标人投标文件的内容一致，并互相补充和解释。

**7 结算原则和支付方式**

7.1 结算原则

7.1.1本项目合同结算价以审计价为准，中标人的中标单价不变，实际工作量以采购人或第三方按照招标文件规定的验收标准核定为准。

7.1.2发生设备维修的，如该设备尚在质保期内的，采购人不另行支付相关费用；如在质保期外的，单价按照投标文件中明确的备品备件单价（含维修人工费）计取，数量按实结算。如投标文件中没有类似备品备件单价可参照的，则由合同双方协商确定维修单价。

7.2 支付方式

7.2.1 本项目合同金额采用**分期付款**方式，在采购人和中标人合同签订，且财政资金到位后，按下款要求支付相应的合同款项。

7.2.2分期付款的时间进度要求和支付比例具体如下：

（1）一笔付款-预付款（30%）：在本合同签订，甲方财政资金下达，中标人提交项目实施方案并经采购人书面确认，采购人收到等额有效的增值税普通发票后向中标人支付合同金额的30%；

（2）第二笔付款-行业验收付款（50%）：项目通过浦东新区行业主管部门组织的行业验收且财政资金下达后，采购人收到等额有效的增值税普通发票后，向中标人支付合同金额50%，但该付款行为不构成对系统的最终验收；

（3）第三笔付款-最终验收付款：项目通过最终验收，财政资金下达后，采购人收到等额有效的增值税普通发票后按审计结果向中标人支付剩余合同款项。

7.3中标人因自身原因造成返工的工作量，采购人将不予计量和支付。

7.4采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时1年期贷款市场报价利率。

三、技术质量要求

**8 适用技术规范和规范性文件**

8.1上海市相关政策

8.1.1 上海市人民政府关于促进综合保税区高质量发展的实施意见。

该意见强调了综合保税区在促进经济发展、吸引外资和推动国际贸易方面的重要性，并提出了多项支持措施，包括土地规划、基础设施建设、政策支持等。这为本项目在保税区内的建设和运营提供了宏观指导和政策支持。

8.1.2 上海市落实《全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案》的实施方案。

该方案针对上海自贸试验区的制度型开放提出了具体措施，包括保税政策的优化、贸易便利化的提升等。其中，对于保税货物的修理和复运出境免征关税、进口葡萄酒和蒸馏酒的特定标签要求等规定，与本项目中涉及的车辆监管和重点货车火车流通环节密切相关。

8.2 上海外高桥保税区相关政策和标准

8.2.1 国务院办公厅关于同意上海外高桥保税区与外高桥港区联动试点的批复。

该批复同意上海外高桥保税区与外高桥港区联动试点，并划定了物流园区的具体范围和四至边界。物流园区享受保税区相关政策，并在进出口税收方面比照实行出口加工区的相关政策。这为本项目在保税区的建设和运营提供了明确的政策依据和区域范围。

8.2.2 上海外高桥保税区的管理规定和监管要求

上海外高桥保税区作为特殊的经济区域，有着严格的管理规定和监管要求。这些规定和要求涉及人员、车辆的出入管理车辆的入出管理、货物的监管和流通、安全保卫等多个方面。本项目的建设必须严格遵守这些规定和要求，确保保税区的正常秩序和安全稳定。

8.2.3 中国（上海）自由贸易试验区保税区域规划环境影响报告书

该报告书对上海自贸试验区保税区域的规划环境影响进行了全面评估，并提出了相应的优化调整和实施建议。本项目的建设需要充分考虑环保因素，确保符合环保要求，避免对保税区域的环境造成不良影响。

本项目的建设依据主要基于上海市及上海外高桥保税区的相关政策和标准。为项目的建设和运营提供了宏观指导和政策支持，还明确了具体的区域范围、管理规定和环保要求。本项目的实施将严格遵守这些依据，确保项目的顺利推进和保税区的持续发展。

8.3 海关总署公告2025年第19号

根据《中华人民共和国海关总署公告2025年第19号》，区域管理政策如下：

8.3.1 货运通道管理强化

承运货物车辆及空载货运车辆，应通过货运通道（常规货 物通道、便捷进出区通道）卡口进出海关特殊监管区域。未经海关同意，车辆或人员不得携带货物通过非货运通道卡口进出海关特殊监管区域。所有载货/空载货运车辆仅允许通过「货运通道」（含常规货物通道、便捷进出区通道）通行，严禁任何单位或个人未经海关书面批准携带货物通过非货运通道（如人员通行通道）。

8.3.2 信息化管理要求

完善卡口通行记录信息库，卡口通行记录信息保存期限不少于3 年，视频记录数据保存期限不少于3个月。

8.4 综合保税区基础和监管设施设置规范

根据进出综保区卡口设施及有关监管设施标准规定：行政卡口及基建物资临时出入口应设置视频监控系统。

8.5 海关综合保税区管理办法（海关总署第256号令）

第三十九条 综合保税区与区外之间进出的交通运输工具、人员应当通过指定通道进出，海关根据需要实施检查。

8.6 公共安全视频图像信息系统管理条例

根据《公共安全视频图像信息系统管理条例》（国务院令第799号）相关规定：

第十四条　公共安全视频系统管理单位应当在系统投入使用之日起30日内，将单位基本情况、公共安全视频系统建设位置、图像采集设备数量及类型、视频图像信息存储期限等基本信息，向所在地县级人民政府公安机关备案。本条例施行前已经启用的，应当在本条例施行之日起90日内备案。公共安全视频系统备案事项发生变化的，应当及时办理备案变更。

公共安全视频系统管理单位应当对备案信息的真实性负责。

公安机关应当加强信息化建设，为公共安全视频系统管理单位办理备案提供便利，能够通过部门间信息共享获得的备案信息，不要求当事人提供。

本项目规划阶段已经征询过浦东公安科技处和保税区公安处意见，不纳管对接本次建设视频，本项目将在系统投入使用之日起30日内按照相关规定完成备案。

8.7 中华人民共和国海关行业标准HS/T 58—2018

该规范全面覆盖海关视频监控系统的设计、实施与维护，强调安全性、兼容性与智能化。

各投标人应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本招标文件中列明，中标人应无条件执行。标准、规范等不一致的，以要求高者为准。

**9 招标内容与质量要求**

9.1 工作量清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目** | **型号及配置** | **单位** | **数量** | **备注** |
| **一** | 流媒体应用相关设备 |  |  |  |  |
| 1 | 卡口抓拍摄像机 | 详见10.2.1 | 台 | 28 |  |
| 2 | 补光灯 | 详见10.2.1 | 台 | 28 |  |
| 3 | 室外高清摄像机 | 详见10.2.1 | 台 | 19 |  |
| 4 | 终端机 | 详见10.2.1 | 台 | 12 |  |
| 5 | 工业交换机 | 详见10.2.1 | 台 | 18 |  |
| 6 | 抱杆机箱 | 详见10.2.1 | 台 | 5 |  |
| 7 | 落地箱 | 详见10.2.1 | 台 | 18 |  |
| 8 | T型监控杆件（含基础） | 详见10.2.1 | 根 | 7 |  |
| 9 | 新增八角杆 挑臂6m | 详见10.2.1 | 根 | 1 |  |
| 10 | 2m延长挑臂Φ50 | 详见10.2.1 | 根 | 2 |  |
| 11 | 光端机 | 详见10.2.1 | 对 | 5 |  |
| 12 | 手井（小） |  | 座 | 21 |  |
| 13 | 手井（大） |  | 座 | 18 |  |
| 14 | Φ76钢管-2孔 |  | m | 462.5 |  |
| 15 | 人行道埋管修复 |  | m2 | 217.5 |  |
| 16 | 绿化带埋管修复 |  | m2 | 60 |  |
| 17 | 电缆YJV3\*2.5 |  | m | 3760 |  |
| 18 | 电缆YJV3\*4 |  | m | 1800 |  |
| 19 | 超五类网线 |  | m | 3760 |  |
| 20 | 线缆及辅材 |  | 点位 | 18 |  |
| 21 | 申请用电 |  | 点位 | 16 |  |
| 22 | PDU | 详见10.2.1 | 台 | 8 |  |
| 23 | CVR存储 | 详见10.2.1 | 台 | 1 |  |
| 24 | 流媒体信息通讯控制设备 | 详见10.2.1 | 台 | 2 |  |
| 25 | 级联汇聚通讯控制设备 | 详见10.2.1 | 台 | 1 |  |
| 26 | 水印叠加模块 | 详见10.2.1 | 台 | 1 |  |
| **二** | 网络相关设备 |  |  |  |  |
| 1 | 汇聚交换机 | 详见10.2.2 | 台 | 2 |  |
| 2 | 视频专网：专线 | 详见10.2.2 | 条 | 1 |  |
| 三 | 安全相关设备 |  |  |  |  |
| 1 | 应用安全网关 | 详见10.2.3 | 套 | 2 |  |
| 2 | SSL VPN网关 | 详见10.2.3 | 套 | 1 |  |
| 3 | 移动安全认证系统 | 详见10.2.3 | 套 | 1 |  |
| 4 | 移动安全认证APP | 详见10.2.3 | 套 | 1 |  |
| 5 | 数据加解密系统 | 详见10.2.3 | 套 | 2 |  |
| 6 | 签名验签系统 | 详见10.2.3 | 套 | 1 |  |
| 7 | 数字证书认证系统 | 详见10.2.3 | 套 | 1 |  |
| 8 | 服务器密码机 | 详见10.2.3 | 台 | 1 |  |
| 9 | 动态令牌认证系统 | 详见10.2.3 | 套 | 1 |  |
| 10 | 堡垒机 | 详见10.2.3 | 台 | 1 |  |
| 11 | IPSecVPN网关 | 详见10.2.3 | 套 | 1 |  |
| 四 | 视频应用设备 |  |  |  |  |
| 1 | 视频数据管理设备 | 详见10.2.4 | 台 | 1 |  |
| 2 | 视频业务管理设备 | 详见10.2.4 | 台 | 2 |  |
| 五 | 软件模块 |  |  |  |  |
| 1 | 监控管理 | 详见10.3.1 | 套 | 1 |  |
| 2 | 平台安全 | 详见10.3.2 | 套 | 1 |  |
| 3 | 智能视觉平台 | 详见10.3.3 | 套 | 1 |  |
| 4 | 数据处理引擎 | 详见10.3.4 | 套 | 1 |  |
| 5 | 海关业务协同 | 详见10.3.5 | 套 | 1 |  |

**说明:上表中所列为本次招标的主要工作因容，投标人不得减少主要工作内容。**

9.2具体技术质量需求

9.2.1建设要求

以实现外高桥保税区行政通道视频全覆盖、重点车辆全智能监管、数据全融合、平台互联互通为目标，建设外高桥保税区域行政通道智能视觉系统，运用人工智能、物联网、大数据等先进技术，搭建外高桥保税区15个出入口智能视觉监管系统，实现可视化智能管理：

* 监管模式跨越：人工查验→智能监管
* 数据能力跨越：分散数据→全域感知
* 防控效能跨越：被动处置→主动预防。

（1）智能视觉监控全覆盖：

全面覆盖：在外高桥保税区15个行政通道出入口部署47台高清智能相机，确保通道全覆盖，实现车辆出入的全方位监控。

高清成像：摄像头具备高清分辨率和低照度成像能力，支持远程调整焦距和视角，适应不同环境和监控需求，确保画面清晰、准确。

夜间监控：摄像头配备夜视补光功能，保证在夜间也能清晰捕捉车辆信息，提升全天候监控能力。

视频存储：建立完善的视频存储系统，对车辆出入视频进行 90 天存储，并保留 3 年的事件信息，方便后期追溯查询和分析。

（2）重点车辆全智能监管：

车型识别：利用智能相机内置 AI 深度学习模型，准确识别大货车、中货车、小货车、大客车、中客车、轿车、面包车、suv、二轮车9种车型。

车牌识别：实现车牌号码的准确识别，支持多种车牌类型，例如蓝牌、黄牌、绿牌、黄绿牌、黑牌、白牌等。

（3）数据全融合：

“一车一档”数据库：建立车辆信息数据库，记录每辆车的详细信息，包括车牌号、车型、进出时间、通道信息、异常行为等，实现车辆信息的全面管理和追溯。

数据安全： 采用数据脱敏、安全审计、加密传输等措施，确保车辆信息的隐私性和安全性。

数据分析：基于“一车一档”数据库，针对特殊时段（如夜间）进出车辆进行数据融合分析，统计出频繁出入的车辆。

数据应用：将车辆信息用于以下方面：

①辆出入监管：实现车辆出入的自动化管理，提高通行效率。

②件预警与处置：对异常行为进行实时预警，提高事件处理效率。

③策支持：为海关等管理部门和决策者提供数据分析和可视化展示，帮助其了解车辆通行情况，优化管理方案。

（4）平台互联互通：

保税区一体化平台：将车辆通行分析后的事件数据传输至保税区一体化平台，实现与平台数据的融合和分析，提升区域治理水平。

跨贸易大数据平台 (保税区域)：将车辆通行分析后的事件结构化数据推送至海关跨境贸易大数据平台，并支持反向主动实时查询，实现数据共享和业务协同，提升海关监管效率和风险防控能力。

数据接口：建立统一标准数据接口，方便未来其他系统或应用调用“一车一档”数据库中的数据，实现数据共享和业务协同。

（5）实施周期及交付要求

自本项目合同签订之日起，中标单位需在25个工作日内完成硬件设备的安装与调试工作，并在3个月内完成软件平台的部署实施。系统部署完成后需进行为期1个月的试运行，以确保软件顺利通过软件测试、安全测试及密评测试，达到项目预期建设目标与质量标准。

9.2.2整体架构概述

外高桥保税区域行政通道智能视觉系统的总体架构是基于先进的信息技术，包括人工智能、物联网、大数据等，旨在构建一个高效、智能、可靠的监控与管理平台。该架构从外场感知层到基础设施层，通过多个支撑层和服务层，实现了对保税区行政通道的全面智能监管。如图1架构图所示，以下是系统总体架构的详细介绍：

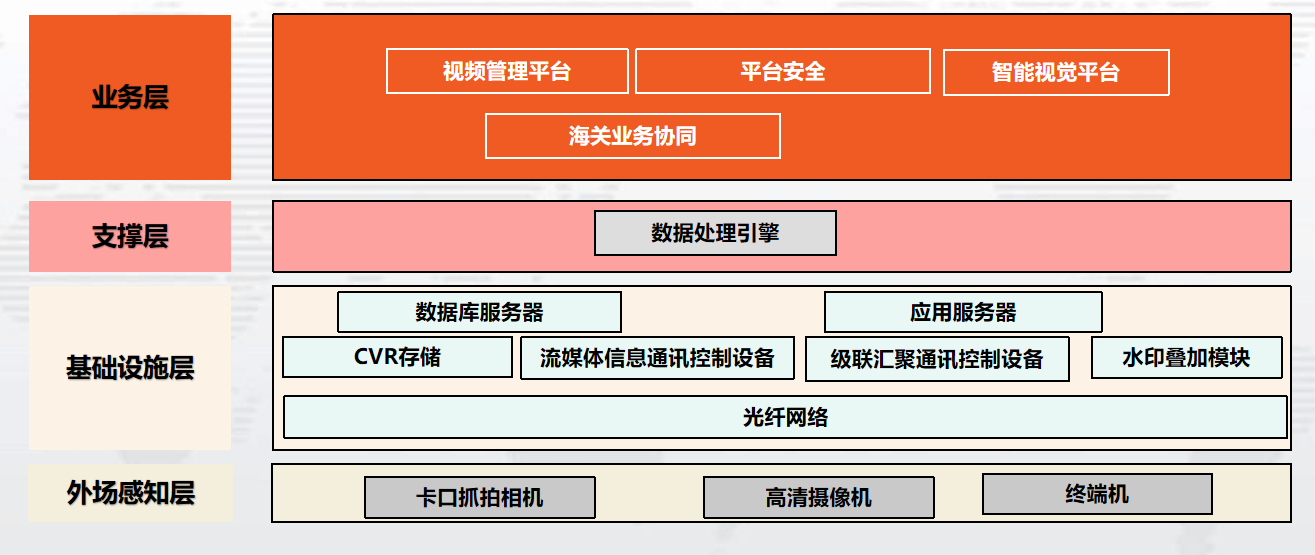


图1 架构图

**10 技术指标要求**

**10.1系统功能与技术指标**

10.1.1 监控管理

监控管理功能作为外高桥保税区域行政通道智能视觉系统的基础性支撑，面向保税区域15个出入口的监控需求，提供视频信号的实时对接与调度，形成完整的视频信息管理能力。该功能以高效的实时响应为目标，可灵活满足不同场景下的监管与应急处置要求。监控管理内容涵盖监控视频资源的统一整合与综合运维，包括但不限于实时画面呈现、录像数据存储管理、监控设备的在线维护、视频画面质量分析、视频资源的统一管理调度以及电视墙集中控制等，充分保障系统运行高效可靠，全面提升保税区域监管和应急指挥能力。

10.1.2 平台安全

平台安全功能以数据安全、系统安全、网络安全、应用安全、物理安全及合规管理为建设目标，构建整体性、多层次的安全保障体系。

在数据与系统安全层面，通过强加密算法保护敏感数据，并采用严格的数据访问控制策略，保障数据仅供授权用户访问。平台用户采用国密算法进行身份验证，并建立角色为核心的权限控制与安全审计机制，确保系统运行与数据操作的安全可靠、过程可追溯。

在网络与应用安全方面，通过安全防护措施加强系统网络安全，包括防火墙部署、入侵检测与实时响应，以及采用安全通信协议进行数据传输。应用系统严格遵守安全开发标准，定期进行代码安全审查、漏洞修复和防病毒管理，持续保障系统免受网络攻击和恶意程序侵害。

在物理安全与合规管理方面，通过严格的服务器物理环境控制以及完善的灾难恢复计划，保障核心设备稳定运行。同时，严格遵守国家和行业的安全法规与隐私保护要求，视频画面中叠加安全标识（OSD），进一步增强平台的安全性和数据的可追溯性。

通过以上安全体系建设，实现对平台运行与数据资源的全面保护，显著提升整体安全防控水平。

10.1.3 智能视觉平台

智能视觉平台依托卡口智能相机，在外高桥保税区域内重要行政通道实现对车辆信息的全结构化采集与分析。系统基于深度学习算法，实时采集包括车牌号码、车型分类、车身颜色及车辆品牌等信息，并支持多种类型车辆的高效识别和准确分类，为区域管理提供可靠的数据支撑。

平台支持在统一的外高桥区域地图上进行监控资源的直观布置与展示，对摄像机、行政通道和监控站点实现精确标记与可视化呈现，有效提升监管效率。同时，平台具备智能化的异常行为分析与风险预警能力，可依据车牌、车型、频次、时段、通道使用情况等数据，自动识别异常车辆行为，实时生成预警信息并触发相应报警动作。管理人员可借助地图直观查看预警事件、快速调取关联视频，并对事件的处理过程和状态进行统一记录管理。平台还提供车辆进出数据的多维度统计分析与报表功能，有效辅助区域交通管理与决策，进一步提升保税区域行政通道的智能监管水平。

10.1.4 数据处理引擎

数据处理引擎作为外高桥保税区域智能视觉系统的数据中枢，具备对外场感知设备采集的视频图像及车辆相关信息的实时处理与管理能力。系统通过合理的存储策略实现数据的分级存储、归档与管理，保障数据的高效利用与历史数据的规范归档。同时，系统针对采集到的数据进行质量监控，确保数据完整性与准确性。依托先进的视频解析与图像识别技术，完成对原始数据的结构化处理，形成标准化的车辆档案信息数据库，有效支撑保税区域行政通道的日常管理、业务决策与合规监管要求。

10.1.5 海关业务协同

海关业务协同功能用于实现智能视觉系统与海关业务平台之间的数据互联互通，提供安全、标准、便捷的数据交换与查询服务。通过统一的接口鉴权机制和访问令牌管理，确保平台间数据调用和信息交互的安全性与合规性。平台能够及时将车辆报警信息及相关事件数据通过符合海关数据标准的接口，向海关跨平台系统实时推送；并可支持海关平台按需主动查询车辆进出区域的历史数据与实时监控画面，便于海关进行合规审查与业务核验。

同时系统具备设备和监控点状态的订阅与通知能力，提供灵活的消息推送模式，有效实现与海关平台的实时联动与动态数据更新。系统采用安全可靠的数据传输通道建设策略，通过多层加密技术确保数据交换过程中的信息安全性，全面满足国家及海关行业对系统信息安全等级保护的合规要求。

**10.2硬件设备参数指标**

10.2.1流媒体应用相关设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备名称 | 规格参数要求 | 数量 | 单位 | 备注 |
| 卡口摄像机 | 包含摄像机、高清镜头、室外防护罩、LED下挂灯、风扇、电源适配器、安装万向节等；  (1) 靶面尺寸≥1/1.2英寸;  (2) 图片分辨率最大支持3840\*2160（不含OSD叠加），字符叠加最大可支持3840\*3184（含OSD叠加)；  (3) 支持主码流同时输出32路3840\*2160、2Mbps、25帧/秒的图像以提供客户端浏览；  (4) 视频帧率支持1帧/秒~50帧/秒可设置；  (5) 支持自动光圈功能，可控制镜头光圈大小来控制曝光；支持快门自适应功能，固定外接镜头的光圈，监控画面支持根据光源亮度变化进行自动调节至正常显示；视频压缩标准支持H.265、H.264、M-JPEG；  (6) 低照度试验：0.00011x（F1.0，帧累积开启，彩色模式），能基本分辨被摄物体的轮廓和色彩；0.00004lx(F1.0，帧累积开启，黑白模式），能基本分辨被摄物体的轮廓。  (7) 支持车辆捕获抓拍功能，在天气晴朗无雾，号牌无遮挡、无污损，白天环境光照度不低于200lx，晚上辅助光照度不高于30lx的条件下测试，白天和晚上的捕获率均≥99.9%  (8) 支持车牌识别功能(含新能源)，在天气晴朗无雾，号牌无遮挡、无污损，白天环境光照度不低于200lx，晚上辅助光照度不高于30lx的条件下测试，白天和晚上的识别率均≥99.9%  (9) 支持车辆上行或下行的行驶方向判断功能；  (10) 支持二轮车（包括摩托车、自行车、电动二轮车）和行人捕获，捕获率白天晚上均≥99%；  (11) 设备支持人脸区域自动曝光，可根据人脸区域和光照变化自动调节人脸区域曝光参数；可通过IE浏览器设置人脸自动曝光的参考亮度、最短持续时间和人脸过滤时间  (12) 支持设定以位置、车速、车型、行驶方向和车牌类型等为触发条件进行抓拍  (13) 支持车辆子品牌识别功能，通过车头可识别7100种，通过车尾可识别3800种，全天识别准确率不低于99%  (14) 支持侧脸过滤功能，过滤的人脸上下、左右角度阈值可设置  (15) 支持人脸目标抓拍头肩照或全景照，模式可选  (16) 支持通过菜单开启或关闭人脸质量优先抓图功能，当开启时，人脸轨迹中人脸质量分数达到设定值时自动进行人脸抓拍  (17) 支持不少于14种车身颜色识别，包括黑、白、灰、红、绿、蓝、黄、粉、紫、棕、青、金、橙、银灰  (18) 支持对二轮车驾驶员、三轮车驾驶员、行人是否佩戴眼镜识别，白天戴眼镜识别准确率不低于99%  (19) 支持检测并跟踪指定区域内不少于200个目标,目标包括机动车、非机动车以及行人等。  (20) 支持1～6 张图片合成一张图片  (21) 感兴趣区域增强编码功能检查：支持24块感兴趣区域(ROI)增强编码功能，ROI区域压缩比0～100可设置  (22) 具有抓拍黄牌车、蓝牌车、绿牌车、渐变绿牌车、黑牌车、白牌车、黄绿双拼牌车和不启用抓拍八个设置选项。可对蓝色、黄色、绿色、渐变绿色、黑色、白色、黄绿双拼色以及其他不同颜色车牌的车辆进行选择抓拍。  (23) 支持对30米处的行人进行人脸抓拍，并可生成分辨率不小于110像素×120像素的人脸图片,图片中人脸两眼瞳距应≥40像素。  (24) 支持检出两眼瞳距12像素点以上的人脸图片。  (25) 支持人脸检测、跟踪、抓拍功能；支持在同一视频画面中，可检测、跟踪不小于 130 个运动人体目标，且抓拍不小于85个运动人脸目标。  (26) 支持车牌黑/白名单设置，最大可设置90万条黑/ 白名单。  (27) 在混合抓拍模式下，人体、非机动车和机动车目标捕获率不低于99%；人脸检出率不小于99%；人脸比对识别率不小于99%；人体抓拍准确率不小于99%。   1. 支持识别车标类型≥460种；在天气晴朗无雾，车辆无遮挡，白天环境光照度不低于200lx，夜晚辅助光照度不高于30lx的情况下进行测试；白天车标识别准确率≥99%；晚上车标识别准确率≥99%。 | 28 | 台 |  |
| 补光灯 | (1) 16颗常亮灯  (2) 光源类型：16颗优质大功率暖光LED  (3) 发光角度40°  (4) 最佳 补光距离16米~26米  (5) 响应时间不大于20us  (6) 支持环境亮度检测，低照度下自动开启  (7) 工作湿度：湿度5%~95%@40℃，无凝结  (8) 电源：220VAC±10%  (9) 功耗：35W MAX  (10) 防护等级：不低于IP66 | 28 | 台 |  |
| 室外高清摄像机 | (1) 主码流支持2560×1440@25fps，子码流支持704×576@25fps，第三码流支持1920×1080@25fps  (2) 具有不小于1/1.8"靶面尺寸。  (3) 最低照度彩色不大于0.0002lx，黑白不大于0.0001 lx。  (4) 内置2.7~13.5mm镜头，支持电动变焦。  (5) 支持H.264、H.265、MJPEG视频编码格式，且具有High Profile编码能力。同一场景相同图像质量下设备在H.264或H.265编码时，开启智能编码和不开启智能编码相比，码率节约≥90%  (6) 在分辨率1920x1080 @ 25fps，码流设置为1Mbps时，视频图像传输延时不大于60ms。  (7) 内置GPU芯片。  (8) 支持周界防范功能，当区域入侵、越界侦测、进入区域、离开区域报警布防开启后，出现行人、非机动车、机动车目标时能触发报警，当检测区域中篮球滚动、小狗移动、树叶晃动及光线明暗变化时不会触发报警。  (9) 支持对两眼瞳距不小于40像素的人脸进行检验。  (10) 支持侧脸过滤功能，可过滤与样机镜头呈上下、左右角度达到预设值的人脸。  (11) 支持抓拍、识别新能源汽车号牌。  (12) 支持声光报警功能，当报警产生时，可在布防时间内联动声音警报和/或白光闪烁。报警声音类型不小于11种，报警音量和重复次数可设置  (13) 设备具有耀光抑制功能，耀光区域≤1%。  (14) 样机采用鳞镜式补光灯，灯杯为半弧形网格鳞片状，其中2颗近光灯、2颗远光灯  (15)灯珠朝向与样机照射方向不同，补光灯开启后正面不可见补光灯灯珠。补光灯开启后灯光均匀无波纹、麻点状、条纹状和不规则亮斑。（如有请提供加盖公章的第三方检测报告）  (16) 需支持IP67防尘防水。内置不少于2个麦克风，1个扬声器，支持3路报警输入，2路报警输出，2路音频输入，1路音频输出，1个SD卡槽，1个RS485接口，支持DC12V或POE供电。 | 19 | 台 |  |
| 终端机 | (1) 支持不少于4个IP摄像机（单路码率10M）的过车记录存储、图片存储、视频存储、数据上传、视频流转发  (2) 可混合接入普通监控用摄像机、智慧监控摄像机、卡口电子警察抓拍机、网络球机等多种前端设备  (3) 坚固紧凑无风扇设计，体积小巧，适合在路边机柜及抱杆机柜使用，单面接口设计，更便于施工操作  (4) 最大支持2TB硬盘存储，图片与录像可设置配额  (5) 触发输入：1个报警输入  (6) 触发输出：1个报警输出  (7) 光纤接口数量：不少于2个  (8) 硬盘盘位数量：不少于1个  (9) USB数量：1  (10) RJ45接口：不少于4个100M以太网接口，不少于2个10/100/1000M自适应以太网接口  (11) RS485接口：1  (12) RS232接口：2  (13) 工作指示灯：4  (14) 视频压缩标准：H.264;H.265  (15) 通用功能：心跳,密码保护，NTP校时  (16) 接入路数：4  (17) 工作温度：温度-30℃~70℃  (18) 工作湿度：湿度5%~95%@40℃，无凝结  (19) 电源：DC12V±10%  (20) 功耗：30W MAX | 12 | 台 |  |
| 工业交换机 | (1) 可用千兆电口数量≥8，可用千兆光口数量≥2  (2) 交换容量≥20 Gbps  (3) 转发性能≥14.88 Mpps  (4) 支持防护等级IP40  (5) 支持≥4K MAC地址表  (6) 支持无风扇设计  (7) 支持双电源输入  (8) 静电放电抗扰度等级（ESD）满足接触放电6kv，空气放电8kv  (9) 网口浪涌等级(Surge)满足6kv  (10) 支持-40℃到+75℃工作环境温度  (11) 提供公安部安全防范报警系统产品质量监督检验测试中心委托检测证书  (12) 提供至少2年原厂维保服务  为保证整体系统稳定性，投标产品尽量与摄像机、解码器、视频综合管理平台为同一品牌 | 18 | 台 |  |
| 抱杆机箱 | 1、抱杆机箱内需预留通信设施(光终端盒、光端机)的安装位置,机箱内线缆布置应整齐、美观、接触可靠,尽量避免交叉;  2、箱体、箱门均采用304不锈钢板,厚度不小于1.5mm;箱内用于安装交换机、电源等附属设施的安装板可采用镀锌板,厚度不小于1.5mm;  3、抱杆机箱制作成型后,表面应平整、无凹陷、压痕、变形等缺陷,箱门开启灵活,侧面百叶窗及散热槽内侧贴防尘薄膜;  4、抱杆机箱上的穿线孔应配置密封垫圈,以防线缆款设时表皮破损,同时防止箱内湖湿;  5、抱杆机箱用不锈钢抱箍国定在立杆中带,控制箱下沿距地面不小于2.5m,抱箍需定制。 | 5 | 台 |  |
| 落地箱 | 1.含防雷、接地、开关电源、检修照明等；  2.机箱材料选用冷扎钢板，机箱表面镀锌后喷飞机灰平光塑，壁厚1.5mm;  3.机箱成型时严格控制焊接变形；  4.机箱顶部必须满焊，不应有漏水和渗水现象出现。 | 18 | 台 |  |
| 杆件钢结构加工及混凝土基础要求 | (1) 钢材:主体构件采用Q235B,其力学性能及碳、硫、磷、锰、硅含量的合格保证必须符合相应标准要求；  (2)焊接材料:手工焊接时Q235B采用E43系列焊条，均为接触满焊;  (3)螺栓:简体法兰连接采用8.8级普通螺栓,其余除注明外均为4.8级普通螺栓,锚栓采用Q235钢;  (4)混凝土:垫层砼为C15.其余采用C25砼.  5)结构主体焊缝均为二级焊缝，需进行超声波验伤，其余焊缝为三级焊缝。  6)施工中如采用进口钢材或代用材料时，需提供该材料的机械性能及化学成分,并进行抽样检查，经设计同意后方可采用。  7)构件出厂前先进行预装，构件制作，放样，安装允许偏差:  (1)构件长度偏差:当总长L≤5m时为+2mm，当L>5m时为+3mm;  (2)构件总体弯曲不大于长度的1/1000,局部弯曲不大于被测长度的1/750:  (3)安装后实际轴线偏离设计位置不得大于所测高度的1/1500.  8)杆件表面做喷塑处理,厚度为80um 颜色为原色(由厂家提供色板进行选择)，加工前需征得建设单位同意后实施。  9)施工时注意结构受风面与基础长边垂直，综合考虑杆件结构、基础方向之间的关系。 | / | / |  |
| 光端机 | 百兆型，1光2电接口 | 5 | 对 |  |
| PDU | 16A航空8口插头公头 | 8 | 台 |  |
| CVR存储 | (1) 设备配置：≥1颗64位多核处理器，≥8GB内存，内存支持扩展到≥256GB，内置SSD固态硬盘（可以扩展到4个SSD作为缓存盘），配置≥8个风扇，风扇支持热插拔并可冗余温控调速；支持热插拔1+1AC220V电源或1+1直流冗余电源供电  (2)设备标配：≥4个2.5Gb网口，支持2个前置 USB2.0接口、2个后置USB3.0接口，支持1个前置VGA接口、1个后置HDMI接口，支持1个RS-232串口，支持4个PCI-E3.0  (3) 具有48个硬盘热插拔插槽；支持硬盘热插拔设备在读写数据时，热插拔设备内的任意块硬盘，设备正常运行不宕机，硬盘不损坏，数据不丢失，业务不中断  (4) 设备具备1个定位灯、1个电源灯、1个设备报警灯、1个就绪灯、1个网络状态灯、1个系统盘状态灯、1个硬盘状态灯，机箱具备防尘滤网，采用双立柱防震设计。设备左右侧面各2个抬手，具备前面板抽拉标签卡  (5) 每个控制单元支持双系统应用，外置系统盘支持RAID1模式，系统盘支持热插拔，当主系统出现故障时，备用系统可接管工作；支持系统盘为独立的2块HDD（SATA、SAS）或SSD盘，组成RAID1  (6) 可接入：2T/3T/4T/6T/8T/10T/12T/14T/16T/18T/20T/25T/26T/30T SATA/SAS硬盘；支持NL-SAS 硬盘、HDD硬盘、SSD硬盘、氦气硬盘、空气硬盘；支持 CMR或SMR硬盘；支持硬盘交错/分时启动  (7) 支持视音频、图片、智能数据流进行混合直存，无须存储服务器和图片服务器的参与，平台服务器宕机时，存储业务正常；支持国际GB/T 28181和Onvif视频流直存模式；  (8) 支持 ONVIF、PSIA、TCP/IP、UDP、SIP、SIP2.0、RTSP、RTP、RTCP、iSCSI、CIFS(SMB)、NFS、FTP、HTTP、AFP、RSYNC、SNMP、IPV4、IPV6、HLS、S3、OSS等协议，支持IP组播  (9) 支持网络RAID纠删码技术，多台存储设备组建网络RAID，设置为负载均衡；单台或多台存储设备组建网络RAID，允许每组RAID中任意1-18个磁盘发生故障，数据不丢失，存储服务不中断；允许每组RAID中任意20块硬盘发生故障，业务不中断  （如有请提供第三方权威机构出具的检测报告证明）  (10) 设备支持版本回退功能，在当前版本出现故障或操作失误后，可进行回退到历史版本，回退后录像正常回放，且历史录像完整  (11) 设备支持MAID2.0磁盘节能功能，当磁盘不工作时，可根据设置的时间自动启动磁盘降速或磁盘休眠指令，降低磁盘驱动能耗  (12) 设备支持硬盘的多级工作模式，包括性能模式、空闲模式（A\B\C，A：硬盘短时空闲，可以正常响应IO；B：较多空闲，磁头不再移动，硬盘满转；C:硬盘完全空闲，磁头不再移动，硬盘降速）、休眠模式（硬盘不再旋转，新下发IO需要唤醒）   1. BMC支持复杂密码，设备首次使用默认密码登录BMC时，提示修改密码，并且需要强制修改完密码后重新登陆，否则无法进入BMC web 2. 存储产品具备国家版权局颁发的系统软件著作权登记证书 | 1 | 台 |  |
| 流媒体信息通讯控制设备 | (1) CPU：配备2颗处理器，单处理器物理核心数≥8核，主频≥3.0 GHz，末级缓存容量≥16 MB，线程数≥16线程，支持内存的最高速率≥3200 MHz，通道数≥2，位宽≥64；  (2) 内存：配置64G DDR4，8根内存插槽；  (3) 硬盘：2块1.2T 10K SAS 硬盘（Raid1），前置最大可选支持12块3.5寸(兼容2.5寸)热插拔SATA/SAS硬盘，板载最大可选支持1个SATA M.2硬盘；  (4) 阵列卡：配置SAS\_HBA卡（支持RAID 0/1/10）；  (5) PCIE扩展：最大支持4个标准PCIE插槽  (6) 网口：标配板载2个千兆电口，支持选配10GbE SFP+等多种网络接口；  (7) 其他接口：标配1个IPMI RJ-45管理接口，位于机箱后部；7个USB 3.0接口 4个位于机箱后部，2个位于机箱前部，1个位于机箱内部；2个VGA接口 1个位于机箱前部，1个位于机箱后部；  (8) 电源：配置550W（1+1）高效铂金CRPS冗余电源； | 2 | 台 |  |
| 级联汇聚通讯控制设备 | (1) CPU：单处理器物理核心数≥24核，主频≥2.2 GHz，末级缓存容量≥64 MB，线程数≥48线程，热设计功耗≥180 W，支持内存的最高速率≥3200 MHz，通道数≥8，位宽≥64；  (2) 内存：配置128G DDR4，16根内存插槽，最大支持扩展至1TB内存  (3) 硬盘：配置2块1.2T 10K SAS硬盘；  (4) 阵列卡：配置SAS\_HBA卡（支持RAID 0/1/10）；  (5) PCIE扩展：最大可选支持6个PCIe扩展插槽；  (6) 网口：4个千兆电口，支持选配10GbE、25GbE SFP+等多种网络接口；  (7) 其他接口：配置1个千兆RJ-45管理接口，4个USB 3.0接口，2个位于机箱后部，2个位于机箱前部；1个VGA口，位于机箱后部；可选1个COM口位于机箱后部；  (8) 电源：配置550W（1+1）高效铂金CRPS冗余电源 | 1 | 台 |  |
| 水印叠加模块 | 【功能特性】  (1) 水印性能：支持对256路1080P@30fps4Mbps叠加水印  (2) 视频安全：提供视频播放叠加水印功能，保证视频码流叠加水印不可擦除，视频外泄后便于用户进行溯源，维护用户视频版权；支持显示水印的展示模板配置。  (3) 展示方式：自定义水印位置、水印布局、水印字体、透明度、水印颜色、旋转角度。  (4) 水印内容：调阅者名称、调阅时间、监控点名称、IP地址及自定义内容。  (5) 服务对象：客户端、上级域平台、平台用户、合作方、解码上墙。  (6) 全面管控：提供用户、监控点、客户端类型、OpenAPI对外开放账号、上级域平台、下级域平台等对象操作实时预览、录像回放、录像下载、云台控制的视频业务权限控制能力，并可对取流路数、时长、使用期限等变量进行调度控制，提升平台视频业务调度的灵活性；支持快速回收监控点视频业务使用权限，并支持添加白名单对象，及时有效防止突发事件外泄。支持多种控制规则的灵活组合，可满足不同项目应用场景需求。  (7) 可视运维：主动采集视频业务数据，呈现监控平台的取流路数、取流流量等业务的管控实时数据和业务数据异常操作的告警提示，并能实时回放平台的监测数据，方便用户回顾分析平台历史运行状态；提供监控链路的数据查询，包括用户、IP、取流业务、监控点名称、操作时间等，便于分析实时管控链路的详情和业务问题的排查追溯；提供管控业务数据的统计分析，便于用户分析平台运行态势及时掌握业务用量，支持报表方式导出统计数据，方便用户做平台视频业务汇报。  【硬件参数】  (1) 处理器：2.8 GHz 8核  (2) 内存：32GB DDR4  (3) 硬盘：256GB SSD  (4) 网络接口：7个10/100/1000M自适应电口，2个10/100/1000M自适应光口  (5) 转码模块：不少于16颗 | 1 | 台 |  |
| 视频数据管理设备 | CPU：12核24线程；  内存：128GB DDR4；  硬盘：480GB固态硬盘；4TB SATA，支持RAID；  满足国产化信创软硬件要求  含国产操作系统 | 1 | 台 |  |
| 视频业务管理设备 | CPU：12核24线程；  内存：128GB DDR4；  硬盘：480GB固态硬盘；10TB SATA，支持RAID；  满足国产化信创软硬件要求  含国产操作系统 | 2 | 台 |  |

10.2.2网络相关设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备名称 | 规格参数要求 | 数量 | 单位 | 备注 |
| 汇聚交换机 | 48口千兆汇聚交换机，8个万兆口  交换机容量：38Tbps/168Tbps  包转发能力：36000Mpps  业务卡槽：3  电源模块：2  支持IEEE 802.1P(CoS 优先级)  支持 IEEE 802.1Q(VLAN)  支持 IEEE 802.1d(STP)/802.1W(RSTP)/802.1S(MSTP)/BPDU 保护支持IEEE 802.1ad(QinQ)，灵活 QinQ和 Van mapping支持 IEEE 802.3x(全双工流控)和背压式流控(半双工)支持IEEE802.3ad(链路聚合)和跨板链路聚合支持 RRPP(快速环网保护协议)  支持跨板端口/流镜像  支持端口广播/多播/未知单播风暴抑制  支持静态 MAC、动态 MAC、黑洞 MAC  支持Jumbo Frame  支持标准和扩展 ACL  支持基于 VLAN 的 ACL  支持Ingress/Egress ACL  支持Ingress/Egress CAR，粒度可达 8Kbps支持 VLAN聚合 CAR，MAC聚合 CAR 功能支持流量整形(Traffic Shaping)  支持 Schedule  支持 802.1P/DSCP 优先级 Mark/Remark  支持层次化 QoS(H-Qos)，支持三级队列调度支持队列调度机制，包括SP、WRR、SP+WRR、WFQ支持拥塞避免机制，包括 Tai-Drop、WRED  支持 Mirroring  支持基于 Layer2协议头、Layer3 协议、Layer4 协议、802.1p 优先级等的组合流分类 | 2 | 台 |  |
| 视频专网专线 | 安全性：需配置防火墙，支持IPSec加密  可用性：SLA不低于99.9%  服务期限：1年  需提供7×24小时故障响应服务  需覆盖15个行政通道出入口部署的47台高清智能相机及机房部署设备； | 1 | 条 |  |

10.2.3安全相关设备

1. 本项目所有设备原厂授权书及7\*24小时3年售后服务承诺函（如有请提供）；
2. 本次项目中的平台软件与密码产品互相兼容；
3. 以下11类投标产品应具备国家密码管理局颁发的有效期内的商用密码产品认证证书，并符合相关国密技术标准（如有请提供产品证书复印件）。
4. 移动安全认证系统、数据加解密系统、数字证书认证系统、动态令牌认证系统、堡垒机应具备与该产品相关的计算机软件著作权登记证书（如有请提供证书复印件）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备名称 | 规格参数要求 | 数量 | 单位 | 备注 |
| 应用安全网关 | 2U设备，支持双电源，国产CPU，支持国产操作系统，不少于8核国产CPUX1，不少于1T硬盘，不少于16G内存，至少支持10个千兆网络接口，支持扩展万兆光纤网口。有独立的MGT和HA网口。  SSL吞吐率（国际）：5Gbps  SSL每秒新建连接数（国际）：4000  SSL吞吐率（国密）：4Gbps  SSL每秒新建连接数（国密）：10000  四层吞吐率：5Gbps  四层每秒新建连接数：800000  四层并发连接数：15000000  七层吞吐率：5Gbps  七层每秒新建请求数：530000  七层并发连接数：2100000  **功能要求：**  支持国密与国际SSL算法套件及协议，支持SSL3.0、TLSv1.0/v1.1/v1.2/v1.3、GMTLSv1.1，支持国密算法套件ECC\_SM4\_SM3、ECDHE\_SM4\_SM3、ECC\_SM4\_GCM\_SM3、ECDHE\_SM4\_GCM\_SM3（对应ECDHE、ECC的算法为SM2）、SM9-WITH-SM4-SM3等算法套件  支持证书自适应，RSA/SM2证书自适应，系统可以在同一个服务实例中配置RSA和SM2两张站点证书并同时启用，根据客户端的算法能力进行自动适应  支持四层、七层负载均衡，支持多种负载算法，包括：轮询、加权轮询（成员、主机）、随机、一致性IP哈希、最快响应、【加权】最小连接数（成员、主机）、【加权】最小流量（成员、主机）、【加权】IP哈希（成员、主机）；  支持多种方式的会话保持、备份会话保持，包括源IP，Cookie，URI，首部，SSLID，插入Cookie，改写Cookie等；  支持会话保持跨虚拟服务器共享、繁忙保护；  支持温暖上线；  支持TCP相关参数的配置。如连接超时，发送超时，读取超时；  支持连接复用；  支持溯源，包括：X-forwarded-For，X-Real-IP；  支持HTTP缓存，压缩；  支持HTTP相关参数配置，包括最大请求头，最大请求体，最大响应头等；  支持WebSocket，HTTP2,HTTP3协议类型；  支持SSL卸载功能，包括：单双向SSL配置，HTTP头部自动修正，会话票据，HSTS，SNI等；  支持多种匹配条件的四层，七层内容交换，包括：源端口，目的端口，源IP，目的IP，HTTP版本，请求方法，URI，首部，Cookie等；  支持多种匹配条件下请求/响应方向的内容改写，基于URL的重定向，基于首部的改写，基于Cookie的改写；  支持多种类型的限制功能，包括：最大连接数限制，最大连接速率限制，最大请求速率限制；  支持浪涌保护机制；  支持自定义故障响应页面；  支持多种类型的健康检查，包括ICMP，TCP,UDP，HTTP,HTTPS，DNS，SMTP等；  支持应用故障自愈合；  支持链路负载均衡，提供针对多出口线路的链路负载，以及链路之间的冗余备份；  智能DNS解析，支持记录A、AAAA、CNAME、TXT、MAIL等记录类型；  同时支持全局负载设备集群和数据中心内服务器负载设备集群两级高可用机制；  支持与负载均衡设备联动，自动发现虚拟服务；  支持DoH功能；  支持完整的DNS服务器功能；  支持完整的LocalDNS功能；  **监控告警：**  支持展示设备启动信息、CPU、内存、磁盘、网口信息、网络信息、证书信息等；支持展示整机的总吞吐和指定网卡的吞吐信息；  支持查看系统CPU、内存、存储、每秒事务数在最近十分钟、最近一小时、最近一天、最近一月的历史状态；  登录系统后查看管理员在线状态，包含登录IP地址、登录时间、登录时长；  支持SNMP对接外部监管平台，支持SNMPv1/v2/v3，支持Trap；  基于虚拟服务，服务池，主机节点的业务流量统计；  支持以邮件或日志等方式，对健康检查状态进行告警  支持管理员的三权分立功能，包括系统管理员、系统操作员、系统审计员；支持自定义管理员角色和权限；  支持基于数字证书认证的UKey方式进行系统管理；也能支持用户名口令认证方式；  支持管理员口令安全策略，可限制登录失败次数、锁定时间、口令有效期、历史重复口令次数、账户锁定策略、关闭口令登录模式；  支持SM2HTTPS、RSAHTTPS访问管理，支持同时启用SM2和RSA在同一端口的HTTPS访问；  支持备份恢复，备份网关所有数据，备份数据使用备份密钥加密，备份密钥保护支持门限秘密共享技术分割备份密钥并将分量存储在UKey中，以及口令保护两种模式，使用UKey进行恢复时使用一半以上UKey即可进行恢复；  支持Web方式的系统远程升级；  支持网卡聚合绑定；  支持VLAN管理，支持动态路由OSPF和BGP管理  管理工具支持Ping、TraceRoute、NSLookup、TCP、WEB等诊断工具，无需登录后台执行；  支持支持双机主备模式部署，支持抢占模式和非抢占模式，支持内外网口主备策略联动  支持N+M集群部署日志外送Syslog服务器； | 2 | 套 |  |
| SSLVPN网关 | 标准机架式设备，国产CPU，冗余电源；  千兆光口≥4个，千兆电口≥6个，支持≥4个万兆光口扩展  性能要求：  SM2每秒新建连接数≥40000  SM2并发连接数≥800000  SM2并发用户数≥800000  SM2吞吐≥8Gbps  SM9吞吐（50并发用户）≥880Mbps  支持国密SM2/SM3/SM4/SM9算法  支持SSL、IPSec两种安全协议  支持SSL3.0、TLSv1.0/v1.1/v1.2/v1.3、GMTLSv1.1，支持国密算法套件ECDHE\_SM4\_SM3、ECC\_SM4\_SM3（对应ECDHE、ECC的算法为SM2）、SM2-WITH-SM4-GCM-SM3套件；  支持B/S应用，支持FTP、Telnet、远程桌面以及通用的C/S应用；  支持创建多个SSL服务，保护HTTP、TCP不同的应用服务；  支持网口的聚合绑定；  支持IPSecNAT穿越；  支持创建VLAN口，聚合网口、BGP/OSPF动态路由、IPv4和IPv6静态路由、GRE等网络相关配置，适配大多数网络场景的部署；  SSLVPN支持地址隐藏功能，系统将真正应用服务的地址隐藏，使用国密算法创建的临时IP地址，且该地址在断开连接时自动消失；  支持不同的服务可拥有不同的站点证书；  支持SSLVPN路由设置、访问控制、在线用户查询等功能。  支持IPSec规则设置、IKE设置、通道设置等功能。  支持防火墙管理，支持白名单管理、ACL规则配置、NAT管理等功能。  支持密码卡管理，提供密码卡信息初始化、RSA密钥管理、SM2密钥管理等功能。（如有请提供第三方检测报告）  支持证书管理，提供签发证书、生成根证书、导入证书、查询等功能，提供新建容器、生成签名证书请求、删除容器等功能。  支持配置告警规则，监控设备系统状态和服务，告警触发时可发送邮件和syslog通知；  支持管理员的三权分立功能，具备系统管理员、系统操作员、系统审计员的用户管理能力；  支持设备自检和报告下载，设备自检项包括算法正确性检测、密钥完整性检测、随机数可靠性检测和设备服务状态检测；  支持对CPU、内存、磁盘容量、SSL代理数、IPSec隧道数、网络吞吐量等资源情况进行实时展示；  支持集群部署，主备机器间自动同步数据，在出现单点故障时主备自动切换，防止单点故障；  支持健康检查，定时检查业务服务器状态，业务服务器出现故障时将流量自动代理到其它正常的业务服务器上；  支持诊断工具，提供运行网络地址、mac地址等功能。  支持日志管理，包括系统日志、访问日志、错误日志、Syslog日志、IPSec日志、SSLVPN客户端日志、SSLVPN服务端日志等 | 1 | 套 |  |
| 移动安全认证系统 | 国产CPU，支持主流Linux操作系统，如RedHat、UOS、麒麟等；  设备高度≤2U，≥2个千兆网口，冗余交流电源；  支持256位SM2公钥密码算法、支持SM2算法协同签名、协同解密；  支持SM3摘要算法；  支持SM4等对称密码算法。  支持SM9算法；  用户服务端部分签名私钥的使用须对用户PIN码和客户端设备信息联合验证通过后方可使用；  支持双证书体系，支持导入CA下发的加密私钥数字信封；  支持加密私钥分割，并加密存储服务端部分加密私钥  服务端程序应实现自身完整性验证；  支持连接第三方CA，为用户申请签发数字证书；  支持验证PKCS1/PKCS7标准格式的电子签名；  支持扫码登录、扫码签名；  支持国密SSL通道；  支持基于数字证书的管理员登录身份认证；  服务端支持单用户粒度的用户密钥备份和恢复功能；  实现协同签名用户的密钥管理，包括密钥查看、更新、销毁等功能；  日志审计管理功能，对协同签名密钥的管理和使用进行审计；  支持用户密钥完整性审计；  服务端应支持密钥归档和密钥周期备份；  支持管理员对设备和密钥强制解绑；  支持用户PIN码错误次数达到上限，则系统冻结用户，管理员可进行解冻；  服务端用户密钥支持PKCS#12密钥证书格式的导入和导出功能；  支持用户密钥使用审计；  支持SNMP监控；  支持license授权；  服务端支持双机或多机集群模式部署；  支持国密SSH、国密FTP；  支持密钥自毁功能、机箱开盖、外置物理装置销毁密钥；  性能参数：  SM2数字签名速度(次/秒)≥17000  SM2签名验证速度(次/秒)≥20000  SM2加密速度(次/秒)≥16000  SM2解密速度(次/秒)≥16000 | 1 | 套 |  |
| 移动安全认证APP | 支持动态口令认证方式，支持基于数字证书的二维码扫码登录  移动端支持Android、IOS、鸿蒙NEXT操作系统  支持移动端证书、动态口令双强度验证； | 1 | 套 |  |
| 数据加解密系统 | 2U机架式设备，国产化CPU；  冗余电源，支持交直流电源输入；  前面板支持液晶屏显示设备信息；  至少提供2个千兆网口、2个万兆网口；  支持SM4、AES对称密码算法；  支持SM3摘要算法；  支持达梦、人大金仓、南大通用、瀚高、OpenGauss、Oracle、MySQL、PostgreSQL等超过15种数据库透明加密，提供国产数据库适配证明材料；  支持字段级加密，确保数据的机密性；  支持字段级完整性保护和校验，确保数据的完整性  加密和完整性保护支持国密算法；；  支持字符、数字、二进制等常见的字段类型；；  支持明文、密文共存模式；  支持存量数据加密洗数；  支持密文数据的解密洗数还原明文；  支持保留格式加密；  支持数据脱敏；  支持自动识别数据库内敏感数据，支持识别常见的身份证号、手机号等敏感数据；  支持用户自定义敏感数据识别规则；  支持对加密字段制定独立于数据库的权限控制策略；  独立权限控制策略支持控制库、表、字段三级对象；  独立权限控制策略至少支持用户/应用对数据库对象的查询权限；  支持以密文列的原始值为条件进行精确查询；  支持密文列的模糊查询；  支持网关透明加密和表空间文件透明加密；  加密和完整性保护对应用无影响，应用无需改造代码即可实现加密和完整性保护  支持数据库管理工具无改造连接数据库加密机进行数据库读写操作  支持仿真模式改写SQL不落库检查改写效果  支持本地密钥管理和连接第三方密钥管理系统两种密钥管理模式  本地密钥管理，密钥生成时采用由内部的密码卡的物理噪声源芯片生成的随机数，密钥生成后由加密卡中的保护密钥加密后存储。  本地密钥管理，支持密钥安全管理，通过管理控制台集中管理所有加密密钥。  支持连接密钥管理系统，由密钥管理系统进行密钥生命周期管理。  支持对密钥及系统配置等重要数据的备份/恢复机制，系统管理员可方便的在管理控制台完成系统备份操作，可下载到本地进行妥善保存。  支持基于HTTPS实现远程管理和配置  支持采用基于数字证书的硬件密码钥匙（USBKEY）“双因子”认证方式实现管理人员的身份鉴别  支持主备高可用机制；  支持系统用户管理，支持根据三权分立原则划分用户角色及权限，包括管理员、审计员、操作员  支持所有的关键操作均记录日志，可对系统中所有的日志进行查询和审计。  支持配置系统网络、系统时间等系统配置。  数据库加密表实时查询速率为：50000条/秒；  数据库加密表实时插入速率：25000条/秒； | 2 | 套 |  |
| 签名验签系统 | 2U机架式设备，国产化CPU。  冗余电源，支持交直流电源输入  前面板支持液晶屏显示设备信息  至少提供2个网络端口  支持万兆网口扩展  投标产品采用的密码板卡、密码芯片，配置的智能密码钥匙，均具备国家密码管理局颁发的有效期内的商用密码产品认证证书，且签名验签系统、密码板卡、密码芯片为同一厂商产品，如有请提供证书复印件。  支持256位SM2公钥密码算法。  支持1024、2048、3072、4096位的RSA公钥密码算法  支持MLDSA、SLHDSA、FALCON、MLKEM等抗量子算法。  支持SM1、SM4等国密对称密码算法。  支持AES、3DES等国际对称密码算法。  支持SM3国密摘要算法。  支持SHA256、SHA384、SHA512国际摘要算法。  证书密钥存储：签名验签服务器内可安全存储各种类型的证书和非对称密钥对；  密钥生成：签名验签服务器可提供各类型非对称密钥的生成功能；  支持基于SM2算法的P1签名、验签  支持基于SM2算法的P7（Attached、Detached）签名、验签  支持基于RSA算法的P1签名、验签  支持基于RSA算法的P7（Attached、Detached）签名、验签  支持基于抗量子算法的P1签名、验签；  支持基于抗量子算法的P7（Attached、Detached）签名、验签；  支持基于SM2算法的数字信封加密、解密  支持基于RSA算法的数字信封加密、解密  支持基于抗量子算法的数字信封加密、解密，如有请提供产品截图证明材料；  签名验签服务器支持集群部署，并支持多机负载；  支持多分区、多服务管理，每个分区独立存储密钥、证书和服务，实现物理隔离，提高服务安全性。  支持基于GM/T 0019《通用密码服务接口规范》标准封装的SDK开发包；可提供C、JAVA接口开发包；  支持应用证书管理，可通过 web 界面进行生成、下载证书请求文件、导入证书、启用、停用等操作  支持配置不同的证书信任域。证书验证策略可配置为不验证、根证书、CRL、OCSP等多种验证策略  支持通过NTP同步系统时间  支持 REST 密码运算服务接口,可通过 web 界面进行 REST 服务管理包括 REST 服务启停token 认证方式、服务证书配置等。  密钥生成时采用由内部的密码卡的物理噪声源芯片生成的随机数，密钥生成后由密码卡中的保护密钥加密后存储。  支持密钥的生成、存储、恢复、销毁等生命周期管理操作，通过管理控制台集中管理密钥整个生命周期。  支持基于https实现远程管理和配置。  支持白名单管理  支持基于SM2、RSA算法的安全通道接入签名验签服务器的密码服务。  支持采用基于数字证书的硬件密码钥匙（USBKEY）“双因子”认证方式实现管理人员的身份鉴别。  支持权限管理：支持根据三权分立原则划分用户角色及权限，包括管理员、审计员、操作员。  支持所有的关键操作均记录日志，可对签名验签服务器所有的操作进行查询和审计。  支持syslog服务，可将业务日志外送至日志服务器。  支持标准SNMP协议，可通过SNMP标准协议监控签名验签服务器的运行状态。  支持 web 界面的设备升级和回滚功能  密钥存储：  SM2密钥对1024对  RSA密钥对1024对  SM2 P1签名/验签：  60000/30000次/秒；  SM2 P7签名/验签：  40000/20000次/秒；  SM2 数字信封加解密：  15000/20000次/秒；  SM2 带签名的数字信封加解密：  9000/9000次/秒；  1024位RSA P1签名/验签：  8800/46000次/秒；  2048位RSA P1签名/验签：  2200/34000次/秒；  1024位RSA P7签名/验签：  8000/34000次/秒；  2048位RSA P7签名/验签：  2000/28000次/秒；  1024位RSA 数字信封加解密：  39000/8400次/秒；  2048位RSA 数字信封加解密：  30000/2000次/秒；  1024位RSA 带签名数字信封加解密：  6600/7000次/秒；  2048位RSA带签名数字信封加解密：  2000/2000次/秒； | 1 | 套 |  |
| 数字证书认证系统 | 标准机架式设备。至少提供2个网络端口，支持万兆网口扩展；  冗余电源，支持交直流电源输入，如有请提供产品照片；冗余硬盘，支持数据冗余备份，如有请提供产品照片；  性能参数：  SDK申请RSA(2048)证书性能:600TPS  SDK查询RSA(2048)证书性能:1500TPS  SDK申请SM2证书性能:6000TPS.  SDK查询SM2证书性能:13000TPS  算法支持：  支持256位SM2公钥密码算法。支持1024、2048、3072、4096位的RSA公钥密码算法。  支持SM1、SM4等对称密码算法。  支持SM3摘要算法。  支持Dilithium、Falcon、SphincsPlus抗量子算法。  支持ECDSA算法.  支持签发RSA、SM2、ECDSA、Dilithium、Falcon、SphincsPlus抗量子算法X509公钥证书，如有请提供产品截图证明  支持通过NTP协议从时间源同步系统时间，保证证书有效期精度到毫秒级。  支持通过WEB控制台实现证书全生命周期管理，包括申请、审核、延期、更新、注销、冻结、解冻和密钥恢复功能；  支持使用遵循CMPv2协议和TCP协议的SDK实现全证书全生命周期管理，包括申请、审核、延期、更新、注销、冻结、解冻和密钥恢复功能；  支持使用遵循restful接口实现全证书全生命周期管理，包括申请、审核、延期、更新、注销、冻结、解冻和密钥恢复功能；  支持业务端支持SSL证书可配,以及支持http协议和https协议；  支持双机负载均衡模式；  支持交叉证书管理，实现与其他CA系统互认:互信功能。  支持自定义证书扩展管理，应对自定义扩展需求。  支持证书模板管理，实现自定义证书模板，支持《GMT·0015-2012·基于SM2密码算法的数字证书格式规范》定义的所有证书扩展。  支持批量证书申请。  支持使用SCEP协议申请数字证书；  支持使用遵循《GMT·0016-2012·智能密码钥匙密码应用接口规范》的智能密码钥匙签发存储数字证书；  支持CRL管理，包括手动签发、自动周期签发CRL发布点等；  支持发布证书、CRL到LDAP服务器；  支持发布证书状态到0CSP服务器；  支持采用基于数字证书的硬件密码钥匙(USBKEY)“双因子”认证方式实现管理人员的身份鉴别。  支持基于https实现远程管理和配置；  支持对数据库的备份管理，系统管理员可方便的在管理控制台完成系统备份操作，可下载到本地进行妥善保存。  支持所有的关键操作均记录日志，可对系统中所有的日志进行查询和审计；  WEB控制台申请证书耗时不超过0.5秒； | 1 | 套 |  |
| 服务器密码机 | 2U机架式设备；具备至少2个RJ-45 10/100/1000Mb的网口；支持1+1冗余电源；硬盘≥1TB；内存≥4GB；信创CPU；MTBF≥50000h  支持IPV4/IPV6双栈协议。具备IPv6ReadyLogo认证证书。  支持SM1、SM2、SM3、SM4、SM7、SM9国密算法，算法模式支持CB/CBC/OFB/CFB/CTR/XTS/GCM/CCM；同时，兼容国际算法RSA、3DES、AES、SHA-1和SHA-2等，具有良好的可扩展性；  具有用户管理功能，对访问用户分级管理，使用智能密码钥匙作为管理介质提高密码设备自身的安全性；按照管理员、审计员、操作员进行管理。  密钥销毁:支持物理的密钥销毁按键，实现在必要情况下的密钥一键销毁功能。  监控界面:WEB界面提供CPU、内存、服务状态等基本使用信息的图形化展示。  支持IP白名单、连接口令等访问控制功能；  内置自签CA功能，支持为连接客户端签发国密数字证书。同时支持第三方证书管理。  日志审计:支持日志的查看、审计以及导出。  产品性能参数：  密钥存储：  非对称密钥对密钥存储(对)≥1024；对称密钥密钥存储(个)≥2048；  256位SM2密钥对生成(对/秒)≥90000；  256位SM2签名(次/秒)≥90000；  256位SM2验签(次/秒)≥30000；  256位SM2加密(次/秒)≥25000；  256位SM2解密(次/秒)≥37000；  SM1算法加解密(Mbps)≥750；  SM4算法加解密(Mbps)≥750；  SM7算法加解密(Mbps)≥800；  ZUC算法(Mbps)≥700；  AES算法加解密(Mbps)≥750；  3DES算法加解密(Mbps)≥650；  SM3杂凑算法(Mbps)≥850；  投标产品采用的密码板卡、密码芯片，配置的智能密码钥匙，均应具备国家密码管理局颁发的有效期内的商用密码产品认证证书，且服务器密码机、密码板卡、密码芯片为同一厂商产品，如有请提供证书复印件 | 1 | 套 |  |
| 动态令牌认证系统 | 支持SM3摘要算法。  支持SM4对称密码算法。  支持动态口令强认证技术，使用密码技术实现的在客户端和服务器之间通过共享秘密进行认证，支持客户端利用口令产生器生成动态令牌。  支持国密标准SM3、SM4算法；  支持手机短信、手机令牌、硬件令牌等认证介质；  支持时间、事件、挑战应答型动态口令  支持与短信网关以及邮件服务器连接实现令牌分发等功能  支持多种认证方式，包括静态口令，动态口令、静态口令+动态口令认证等；  支持通过Radius协议以及LDAP协议实现动态或静态密码验证  提供配套的客户端控件，实现动态密码服务器与微信小程序、Android、iOS等操作系统联动；  支持对外提供API接口，通过API接口可以进行验证、管理等操作；  支持提供独立管理页面：用户管理、令牌管理、日志管理等  支持权限管理，可以为不同的管理人员分配不同的管理权限  支持企业管理，可以将用户、令牌等资源进行分组织机构  支持令牌生命周期管理、令牌PIN码使用错误次数达上限自动冻结等功能  用户令牌信息包括用户名、令牌名、令牌种类、设备ID、绑定时间，可以进行绑定解绑操作；  支持账号集中管理功能，以及LDAP、AD同步账号数据功能；  支持提供日志转发到第三方Syslog服务功能；  支持日志分类记录，生成、验证、管理、以及其他的相关日志，并在web页面可查看；  支持系统后台审计管理员操作日志  能够对口令验证、验证服务器连接数、验证服务器活动连接数、数据库连接池大小、数据库链接剩余大小等指标进行监控统计；  服务端支持双机或多机集群模式部署。  支持多种数据库，包括dm、My SQL、Postgres等。  支持IPV4\IPV6双栈协议  最大用户数≥200000，响应性能≥3000TPS | 1 | 套 |  |
| 堡垒机 | 物理旁路单臂部署，以逻辑网关方式工作，不改变现有网络结构。  客户端到堡垒机之间仅开放单一端口（如443）即可实现堡垒机的管理、运维、审计的全部功能。  支持基于web的配置管理、操作审计。  支持基于web的运维操作、包括文本协议ssh/telnet，图形协议rdp/vnc/x11、常见数据库和多种国产数据库。  支持secureCRT 等ssh客户端软件直接登录运维，进行ssh/telnet文本类协议访问操作。  支持secureFX 等sftp客户端软件直接登录运维，进行sftp协议访问操作。  支持集群部署，具可扩展性，方便后期动态扩容；  新部署系统可以直接加入集群，无需任何其他复杂配置。  支持集群多节点负载均衡，对外提供统一的访问IP。  通过统一的IP访问操作，各工作节点自动分担访问流量。  支持数据库双主环境，自动数据同步备份；  支持数据库运行状态自动检测，随时掌握双主同步状态是否正常；  支持层级组织管理；  支持管理的用户、资源等，关联到具体的组织节点。  可限制用户仅能对本组织及下级组织范围的资源进行管理和访问操作。  灵活划分角色权限，可根据业务模块自定义角色权限，控制可操作的业务模块范围；  一个用户可同时拥有多个角色。  内置角色需包括：系统管理员、权限管理员、操作员与审计员。  投标产品支持静态口令、动态口令、AD域、LDAP、Radius、国密ukey、短信、指纹等多种认证方式；  支持静态口令、动态口令、AD域、LDAP、Radius、国密ukey、短信、指纹任意两种组合的双因子认证。  认证因素含静态口令时，静态口令有有效期限制和使用次数限制，口令到期前会有到期提醒；  口令到期或用户成功登录次数达上限时会强制要求改密；  管理员注册用户时指定了用户口令，用户首次登录成功后强制要求改密。  用户登录达一定次数后用户会被锁定，一段时间内不允许再次登录，到期自动解锁。  设备自身集成一次性口令认证服务器模块，或能对接专用的OTP动态口令认证系统；  支持手机软件程序APP。  支持用户的批量导入、导出和批量的修改维护如批量禁用、批量解锁，批量加入用户组等操作，方便快速部署。  用户可自行维护个人基本信息（如真实姓名、联系方式）；  用户可自行修改自己的登录静态口令；  用户可自行维护个人偏好配置，如运维操作默认使用的工具类型。  支持用户自注册，从页面发起注册申请，管理员审批后可登录访问系统；  管理员可对自注册申请进行批量审批；  管理员可配置是否允许个人注册用户，支持定义自注册可选认证类型。  支持用户组管理；  用户可加入到一个或者多个用户组。  支持windows/linux/UNIX/网络设备类资源管理。  支持常见数据库类资源管理。  支持业务应用类资源管理。  支持各类访问协议的默认端口。  支持自注册数据库类型。  支持配置资源的所属设备名、操作系统类型、IP地址、协议类型、访问端口等属性。  支持注册操作系统类型及版本。  支持配置操作系统专用的帐户管理操作模板。  支持手动资源添加。  支持通过模版批量导入资源。  支持通过 API 接口，由第三方系统导入资源。  支持配置资源的登录帐户使用资源所在操作系统帐户、外部认证设备上的帐户（AD、LDAP等）、以及资源私有帐户。  Windows系统资源，支持配置windows帐户管理方式：smb、部署agent的方式（hacsync、winuser）；  支持通过设定ip段扫描存在的资源和标准端口，可以自动或者审核后纳管到堡垒机；  支持通过vcenter、exsi系统API接口扫描虚拟资源，可以自动或者审核后纳管到堡垒机。  支持设备组管理；  支持单一资源可加入多个设备组；  支持设备组删除，保留资源不变。  支持自注册应用发布类资源类型；  支持为自注册的应用发布类资源类型配置自动登录模板  支持纳管资源的批量导出。  支持第三方系统接入，如OA系统、ITSM、CMDB等  支持接入应用的认证、授权配置，授权包括可访问接口、允许获取授权帐户列表的时间段、以及是否推送帐户信息到应用等。  支持对纳管设备的连通性校验；  支持单个设备校验与批量校验；  支持特定协议端口连通性校验。  支持资源更新，变更资源的IP地址、关联访问协议、协议服务端口等。  支持对不再使用资源的进行删除操作。  支持纳管Unix/Linux/Windows操作系统帐户；  支持纳管AD域、LDAP帐户；  支持纳管MySQL、Oracle、SqlServer、DaMeng、DB2、PG等常见数据库帐户；  支持纳管juniper、华三、华为、CISCO网络设备帐户；  支持WebLogic、Was等中间件管理帐户。  支持各类帐户注册；  支持各类帐户的批量导入方式注册，方便快速部署；  帐户注册时，可选择帐户托管，自动对注册的帐户执行改密操作；  对已注册的未托管帐户，支持批量托管操作。  支持Windows/windows Server、AIX/UNIX/Linux等操作系统帐户、数据库帐户、中间件帐户自动发现；  支持帐户监控，对识别到的帐户增加、删除变更发送邮件通知；  支持自动发现的帐户自动注册到堡垒机。  支持在目标服务器上添加帐户，包含：Unix/Linux/Windows操作系统，  MySQL、Oracle、SqlServer等常见数据库,WebLogic、Was等中间件帐户；  支持各类帐户的批量导入方式添加，方便快速部署；  帐户添加时，可选择帐户托管，此后自动对添加帐户执行改密操作；  帐户添加时，可手动录入密码，或者随机生成复合口令策略强度的密码；  支持将已经纳管的帐户从系统注销；  支持批量勾选和批量导入方式，进行快速注销；  支持将已经纳管的帐户从目标服务器删除；  支持批量勾选和批量导入方式，进行快速删除；  完整的帐户日志，包括帐户的管理操作、改密操作、口令领用操作、运维自动登录操作记录。  支持帐户的启用/禁用操作；  被禁用的帐户不允许被执行运维访问登录代填、口令明文领用操作  帐户采用专用安全终端设备(终端密钥分发器)进行备份  支持帐户分组管理；  帐户可同时属于多个分组。  支持自定义口令策略， 包括密码长度、包含各类字符的数量、与旧密码相似的程度、禁用字符等  支持自定义改密策略，包括改密周期、改密时间、口令被使用后自动改密及改密时间窗口等  自持自定义弱密码策略，包括密码长度、组成密码的各类字符个数、逻辑连续字符数、键盘连续字符数、单字符最大出现次数、口令包含帐户名等  支持操作系统关联绑定口令策略、改密策略  支持纳管设备关联绑定口令策略、改密策略  支持纳管帐户关联绑定口令策略、改密策略  支持基于帐户类型、帐户级别组合关系关联口令策略、改密策略  系统支持默认口令策略、改密策略；  上述各类关联策略均不存时，使用默认口令策略、改密策略  支持Windows/Linux/UNIX 操作系统帐户口令校验；  支持AD域/LDAP/RADIUS帐户口令校验；  支持华为、H3C、CISCO等网络设备帐户口令校验；  支持mysql，oralce、sqlserver、db2、pg、dmeng等常见数据库帐户口令校验；  支持WAS、WebLogic等中间件帐户口令校验。  帐户注册时， 支持选择对口令校验不通过的帐户允许注册或禁止注册。  支持对已纳管的帐户进行口令校验操作。  支持对已纳管帐户进行口令校验修正操作。  支持建立周期性口令校验计划任务，定时执行帐户口令校验操作。  支持Windows/Linux/UNIX 操作系统帐户口令更新；  支持AD域/LDAP/RADIUS帐户口令更新；  支持华为、H3C、CISCO等网络设备帐户口令更新；  支持mysql，oralce、sqlserver、db2、pg、dmeng等常见数据库帐户口令更新；  支持WAS、WebLogic等中间件帐户口令更新  支持对不允许直接登录访问的帐户执行口令更新操作。  支持托管帐户按改密策略执行周期/定时口令更新操作。  支持建立周期性口令更新计划任务，定时执行帐户口令更新操作。  口令更新支持使用管理员帐户重置口令；  口令更新支持使用帐户自身更新口令。  系统支持保留完整的历史密码表，以便出现故障，问题时进行口令恢复  支持口令修改操作，将涉及变更的帐户邮件通知管理员。  支持注册帐户基于弱密码策略的弱口令校验。  支持建立周期性口令更新计划任务，周期/定时执行帐户弱口令校验操作。  支持弱口令校验结果邮件发送管理员。  支持等级帐户ssh访问认证密钥；  支持ssh访问认证密钥校验；  支持ssh访问认证密钥更新。  **安全要求：**  提供初始化国密计算服务功能，可灵活选择国密计算服务，可以通过内置密码卡、外部密码机、密码服务平台作为安全计算源。  提供成熟的合规模板供选择，覆盖密评设备与计算环节对堡垒机的相关要求。  提供合规模板的灵活调整功能，可对启用的合规模板基线按企业自身需要进行灵活调整。  对用户登录堡垒机的认证凭据等敏感信息加密存储。  对访问目标资源的帐户口令等认证凭据加密存储。  堡垒机自身访问数据库的用户名、认证口令加密存储。  采用国密Ukey或者动态令牌满足身份鉴别国密的要求。  通过https访问，同时兼容国密和国际链路SSL，自适应国密和国际浏览器。  可配置用户登录访问堡垒机的控制规则，指定用户在什么时间范围、什么IP范围可登录堡垒机。  登录堡垒机用户的访问控制信息采用国密算法实现其完整性校验；  操作员通过堡垒机运维的录像文件做完整性校验，防止被篡改，每条会话单独的录像单独校验；  堡垒机的升级补丁需采用国密算法的完整性校验机制，确保升级补丁文件的完整性。  一键生成合规报告并可导出，针对密评可按密评DAK量化评估框架对密评实现状况进行量化评估；  **信创/国产化支持：**  操作系统默认使用openEuler；支持使用UOS/银河麒麟 等在信创名录的操作系统  默认采用mysql5.7/8.0版本数据库，支持使用mysql、PG数据库或DM、VAST等国产数据库。  支持通过信创终端（麒麟、统信、EulerOS等），使用浏览器登录和管理所有堡垒机功能。  支持通过信创终端（麒麟、统信、EulerOS等），使用浏览器登录和运维所有服务器。  支持通过信创终端（麒麟、统信、EulerOS等），使用浏览器登录和审计所有通过堡垒机的管理和运维操作。  支持调用本地（windows、统信、麒麟、Euler终端）的数据库运维工具dbeaver实现对数据库mysql、oracle、db2、达梦、pg、高斯、神通数据库的运维和审计。  支持Windows ADS应用发布，通过应用发布浏览器运维BS服务以及数据库dbeaver运维访问数据库。  同时支持信创应用发布、windows 应用发布、终端应用发布，运维时可以选择不同的模式进行运维访问操作。  性能参数：  管理资源数量：可管理不低于 1000 个用户；  可管理不少于 2000 个设备资源；  可管理不低于 10000 个帐户。  文本并发性能：可支持 2000 文本协议运维访问并发。  Rdp并发性能 可支持600 RDP图形协议运维访问并发。 | 1 | 套 |  |
| IPSecVPN网关 | 标准机架式设备，冗余电源；  千兆光口≥4个，千兆电口≥6个，支持≥4个万兆光口扩展  性能要求：  ipsec密文吞吐率≥3.2Gbps  ipsec最大并发隧道数≥74000  支持国密SM2/SM3/SM4/SM9算法  支持SSL、IPSec两种安全协议  支持SSL3.0、TLSv1.0/v1.1/v1.2/v1.3、GMTLSv1.1，支持国密算法套件ECDHE\_SM4\_SM3、ECC\_SM4\_SM3（对应ECDHE、ECC的算法为SM2）、SM2-WITH-SM4-GCM-SM3套件；  支持B/S应用，支持FTP、Telnet、远程桌面以及通用的C/S应用；  支持创建多个SSL服务，保护HTTP、TCP不同的应用服务；  支持网口的聚合绑定；  支持IPSecNAT穿越；  支持创建VLAN口，聚合网口、BGP/OSPF动态路由、IPv4和IPv6静态路由、GRE等网络相关配置，适配大多数网络场景的部署；  SSLVPN支持地址隐藏功能，系统将真正应用服务的地址隐藏，使用国密算法创建的临时IP地址，且该地址在断开连接时自动消失；  支持不同的服务可拥有不同的站点证书；  支持SSLVPN路由设置、访问控制、在线用户查询等功能。  支持IPSec规则设置、IKE设置、通道设置等功能。  支持防火墙管理，支持白名单管理、ACL规则配置、NAT管理等功能。  支持密码卡管理，提供密码卡信息初始化、RSA密钥管理、SM2密钥管理等功能。  支持证书管理，提供签发证书、生成根证书、导入证书、查询等功能，提供新建容器、生成签名证书请求、删除容器等功能。  支持配置告警规则，监控设备系统状态和服务，告警触发时可发送邮件和syslog通知；  支持管理员的三权分立功能，具备系统管理员、系统操作员、系统审计员的用户管理能力；  支持设备自检和报告下载，设备自检项包括算法正确性检测、密钥完整性检测、随机数可靠性检测和设备服务状态检测；  支持对CPU、内存、磁盘容量、SSL代理数、IPSec隧道数、网络吞吐量等资源情况进行实时展示；  支持集群部署，主备机器间自动同步数据，在出现单点故障时主备自动切换，防止单点故障；  支持健康检查，定时检查业务服务器状态，业务服务器出现故障时将流量自动代理到其它正常的业务服务器上；  支持诊断工具，提供运行网络地址、mac地址等功能。  支持日志管理，包括系统日志、访问日志、错误日志、Syslog日志、IPSec日志、SSLVPN客户端日志、SSLVPN服务端日志等 | 1 | 套 |  |

**说明:上表中所列为本次招标的主要工作因容，投标人不得减少主要工作内容。**

**10.3软件技术方案**

10.3.1监控管理

在主应用及支撑平台的开发需求中，通道视频直连直调是确保外高桥保税区域行政通道智能视觉系统高效运行的关键功能之一。该功能旨在实现保税区15个出入口监控视频的实时、直接连接与快速调取，为管理人员提供即时、直观的监控画面，以应对各类突发情况和日常监管需求。

10.3.1.1实时图像点播

支持取流重连次数和重连时间间隔配置；支持视频解码模式切换（硬解/软解）；支持预览一键切换到回放和一键上墙；支持多种画面分割模式（包括个性化分割和走廊分割）；支持辅屏预览、批量关闭预览窗口、窗口自适应和全屏播放等功能；支持监控点预览画面抓图、声音控制、电子放大、主子码流切换、码流信息查看等操作；支持预览工具栏自定义配置；支持紧急录像和即时回放；支持限时预览功能。

10.3.1.2历史图像的检索和回放

支持对历史视频录像的查询、播放、画面流控、片段下载等功能。

10.3.1.3设备网络管理

对接入平台的视频设备进行在线巡检，及时发现故障设备和掉线设备；支持监控点通道、录制状态、录像完整性、录像保存天数等指标检测；支持告警信息统计展现和告警阈值配置；提供视频运维报表统计能力。

10.3.1.4视频质量诊断

提供视频图像诊断和监测服务，支持多种图像质量诊断指标（如模糊、过亮、偏色等）；支持码流分辨率、编码格式指标采集；支持诊断对比图查看和结果矫正功能；支持巡检计划配置。

10.3.1.5视频上墙

支持电视墙场景管理和上墙控制，实现场景一键上墙、场景切换、电视墙切换、监控点上下墙、轮巡控制等操作。

10.3.1.6资源管理

支持基础目录和业务目录的创建和管理；支持在目录下创建区域树，支持区域的导出和导入；支持设备管理（编码设备、报警设备、人证设备等）和通道管理。

10.3.1.7通用配置

包括用户登录配置、视频配置、页面水印设置、图片存储配置、视频存储配置、文件存储配置、设备校时、全局配置等。

10.3.2平台安全

10.3.2.1 国密app扫码登录

采用国密app扫码认证机制，确保系统用户的身份真实性。

10.3.2.2用户权限管理

建立细粒度的权限控制体系，根据用户角色分配不同的操作权限。

实施严格的数据访问控制策略，确保只有授权用户才能访问敏感信息。

10.3.2.3日志管理

记录所有用户的操作日志，定期进行安全审计，以便于追踪和监控潜在的安全威胁。

10.3.2.4图像OSD标识

在视频图像中嵌入字符标识，提高视频的安全性和可追溯性。

10.3.2.5数据加解密

确保所有敏感数据，包括车辆信息、视频监控数据等，在存储过程中采用强加密算法进行加密。

10.3.3智能视觉平台

通过部署卡口智能相机的方式在外高桥保税区域各行政通道每2车道辐射一台网络摄像机，支持视频触发并实现全结构化：通过加载深度学习算法，支持多目标混合场景应用，支持机动车辆抓拍，内置车牌识别、车身颜色识别、车型识别功能，车辆主子品牌识别功能。

10.3.3.1 外高桥区域地图建设

在外高桥区域地图上合理布置摄像机、行政通道和站点等监控设备，以提高监控效率和管理水平。

10.3.3.2 摄像机、通道、站点等撒点

根据外高桥区域的安全需求和监控目标，在地图上撒点标注所有网络摄像机、行政通道和站点。

10.3.3.3 车辆查询

支持对卡口抓拍机抓拍的车辆进行查询，包括车牌号码、车牌图片、通过时间、车辆图片等详细信息。

10.3.3.4 报警设置

基于海关标准HS/T 58—2018，平台需提供灵活可配置的报警规则引擎，满足多场景风险预警需求：

10.3.3.5 ‌异常行为分析并报警‌

为了保障保税区的安全，系统还需具备车辆异常行为检测分析功能。异常行为包括但不限于特殊时段（如夜间）频繁进出区、违规通过行政通道进出保税区的货运车辆（如厢式货车，集卡）、车辆行政通道未出区即二次进入‌（跨通道混走）情况识别并抓拍检测等。系统应能够实时监测车辆的通行情况，对异常行为进行预警和记录。

对车辆车牌、车型等结构化数据进行分析监控异常行为。

提供进出通道、时间、频次等分析维度帮助识别潜在风险和问题。

10.3.3.6 ‌报警记录‌

记录报警事件完整信息，包括报警源（设备ID/名称）、报警级别、触发时间、处理状态（未处理/已处理）、处理人及备注。

支持按时间轴查看报警事件流，并关联摄像头抓拍图片、视频片段作为证据链。

对接日志审计系统，满足海关合规性审查要求。

10.3.3.7 ‌报警事件撒点‌

报警事件自动标注于地图（如货车违规、频次异常）。

点击事件点可查看详情（车牌、时间、关联摄像头），支持快速定位周边监控资源。

10.3.3.8 ‌报警视频切换‌

报警触发时，值班人员可通过地图或事件列表直接跳转至关联摄像头实时画面支持视频报警联动切换，提高应急响应速度。

10.3.3.9 ‌报警筛选查询‌

按报警类型（频次异常、车辆违规）、通道点位、处理状态、时间范围等组合查询。

10.3.3.10 ‌可视化报表‌

对车辆出入数据进行统计分析，生成车辆出入报告，为交通管理提供决策支持。如：‌流量分析‌：各卡口分时段车流量统计（柱状图/折线图），识别高峰时段。

10.3.4数据处理引擎

10.3.4.1 数据采集

实时采集外场感知设备的视频图像和相关信息（如车牌、车型、颜色、时间等）。

10.3.4.2 数据存储

采用分级存储策略，对采集到的数据进行高效存储和管理。

10.3.4.3 数据质量管理

对采集到的数据进行质量监控和管理，确保数据的完整性和准确性。

10.3.4.4 数据结构化

采用先进的视频解析技术和图像处理算法，对视频图像进行解析和识别，提取出车牌、车型、颜色等结构化信息，并构建“一车一档”数据库。

10.3.4.5 数据归档与合规性

按业务需求设置归档策略，对历史数据进行归档管理，并确保数据操作的合规性。

10.3.5海关业务协同

10.3.5.1 统一鉴权‌

‌鉴权流程‌：

第三方系统调用接口前，需通过OAuth 2.0协议获取访问令牌，令牌需关联角色权限（如只读、读写）。

支持IP白名单限制，确保接口仅对授权服务器开放。

10.3.5.2 报警信息跨平台推送‌

‌数据传输‌：

通过保税区三级等保认证通道，以JSON格式实时推送报警事件（含车牌、时间、位置、抓拍图）。

异常重传机制：网络中断时缓存未成功数据，恢复后自动补发，确保数据完整性。

‌接口规范‌：

提供RESTful API，支持同步/异步响应模式，定义明确的状态码与错误信息。

10.3.5.3 海关主动查询功能‌

‌查询逻辑‌：

支持按“车牌号+时间段”组合查询，返回车辆在所有通道的进出记录（如2号门进、3号门出）。

结果包含抓拍图片、视频片段链接（需鉴权访问），供海关进一步核查。

10.3.5.4 资源获取‌

‌基于GB/T 28181-2016标准，提供设备信息查询、历史录像下载接口。

视频片段下载支持按起止时间截取，并附加国密水印（含下载者ID、时间戳），防止篡改。

10.3.5.5视频取流‌

‌基于GB/T 28181-2016标准，提供实时视频流获取接口。

按角色控制可访问的监控权限。

10.3.5.6订阅和通知‌

第三方可批量订阅设备/监控点状态（在线/离线），支持Webhook回调或消息队列（如Kafka）接收通知。

提供订阅生命周期管理（创建、修改、删除），避免无效订阅占用资源。

10.3.5.7加密传输通道建设‌

数据传输层采用IPsec VPN隧道加密，应用层叠加国密算法（SM4加密、SM3摘要）。

通过国家密码管理局认证，满足海关信息系统三级等保要求。

**10.4软件性能指标**

10.4.1实时图像点播

视频实时点播响应时间：≤3秒；

并发视频实时预览数量：≥10路

视频解码切换延迟：≤2秒；

视频取流重连成功率：≥95%。

10.4.2历史图像检索回放

历史视频检索响应时间：≤5秒；

并发视频回放数量：≥10路；

单路历史视频回放流畅性：播放卡顿次数≤5次/小时。

10.4.3设备网络管理

视频设备巡检周期：≤10分钟；

设备掉线报警响应时间：≤30秒；

运维报表生成时间：≤20秒。

10.4.4视频质量诊断

诊断巡检周期：≤30分钟；

图像质量诊断准确率：≥95%；

图像质量问题报警延迟：≤2分钟。

10.4.5视频上墙

视频上墙切换响应时间：≤3秒；

同时上墙视频数：≥9路。

10.4.6资源管理

区域目录树加载响应时间：≤5秒；

设备批量导入/导出（100台以内）处理时长：≤30秒。

10.4.7地图及设备撒点

地图加载响应时间：≤5秒；

撒点设备信息展示延迟：≤3秒。

10.4.8车辆管理与查询

单次车辆查询响应时间：≤5秒；

并发车辆查询能力：≥20次/秒。

10.4.9报警管理

实时报警触发和通知延迟：≤5秒；

异常行为分析准确率：≥90%；

并发报警处理能力：≥50条/秒。

10.4.10可视化报表

车辆流量报表生成响应时间：≤5秒；

数据刷新周期：≤15分钟。

10.4.11数据采集

数据采集延迟：≤3秒；

数据采集吞吐能力：≥100条/秒。

10.4.12数据存储

视频数据存储延迟：≤3秒；

数据存储吞吐能力：≥100MB/s。

10.4.13数据质量管理

数据质量巡检周期：≤15分钟；

数据异常报警延迟：≤2分钟。

10.4.14数据结构化

视频结构化处理延迟：≤5秒；

车辆结构化数据准确率（车牌、车型、颜色）：≥95%；

结构化数据处理能力：≥20条/秒

10.4.15数据归档

数据归档处理速度：≥20GB/小时；

归档数据检索响应时间：≤5秒。

10.4.16统一鉴权

OAuth 2.0鉴权响应时间：≤3秒；

IP白名单校验准确率：≥99.9%。

10.4.17报警信息跨平台推送

报警信息推送延迟：≤5秒；

异常数据重传补发延迟：≤20秒（网络恢复后）。

10.4.18海关主动查询

单次查询响应时间：≤3秒；

并发查询处理能力：≥10次/秒。

10.4.19视频资源获取与取流

实时视频取流延迟：≤5秒；

并发视频取流能力：≥10路。

10.4.20订阅通知

设备状态通知延迟：≤5秒；

消息推送能力：≥50条/秒。

10.4.21加密传输通道

数据传输加解密延迟：≤100毫秒；

通道可靠性：≥99.99%。

**11质量标准和验收方案**

11.1质量标准

11.1.1 中标人所交付的信息系统应满足本项目合同文件明确的功能性、使用性要求。信息系统的质量标准按照国家标准和招标需求确定，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合招标目的的特定标准确定。

11.1.2 中标人所交付的信息系统还应符合国家和上海市有关系统运行安全之规定。

11.2系统测试及验收方案

11.2.1 采购人应依据信息系统项目工程的条件和性质，按照招标文件明确的要求向中标人提供信息系统的施工、安装和集成环境。如采购人未能在该时间内提供该施工和安装环境，中标人可相应顺延交付日期。如对中标人造成经济损失，采购人还应依本合同规定承担违约责任。

11.2.2中标人应负责系统及系统设备在实施现场就位安装和调试、操作培训等的全部工作，按照合同文件工作与管理要求负责对项目进度的安排、现场的安全文明施工统一管理和协调，严格遵守国家、本市安全生产有关管理规定，严格按安全标准组织项目实施，采取必要的安全防护措施，消除安全事故隐患。由于中标人管理与安全措施不力造成事故的责任和因此发生的费用，由中标人承担。

11.2.3系统具备隐蔽条件或达到中间验收部位，中标人进行自检，并在隐蔽或中间验收前48小时以书面形式通知采购人、监理验收。通知包括隐蔽和中间验收的内容、验收时间和地点。中标人准备验收记录，验收合格，监理工程师在验收记录上签字后，中标人可进行隐蔽和继续施工。验收不合格，中标人在工程师限定的时间内修改后重新验收。

11.2.4 中标人应在进行系统交付前5个工作日内，以书面方式通知采购人并向采购人提供完整的竣工资料、竣工验收报告及竣工图。采购人应当在接到通知与资料的5个工作日内安排交付验收。中标人在交付前应当根据合同文件中的检测标准对本项目进行功能和运行检测，以确认本项目初步达到符合本合同交付的规定。

11.2.5中标人应按照合同及其附件所约定的内容进行交付，如果约定采购人可以使用或拥有某软件源代码的，中标人应同时交付软件的源代码并不做任何的权利保留。所交付的文档与文件应当是可供人阅读的书面和电子文档。

11.2.6 采购人在本项目交付后，应当在5个工作日内向中标人出具书面文件，以确认其初步达到符合本合同所约定的任务、需求和功能。如有缺陷，应向中标人陈述需要改进的缺陷。中标人应立即改进此项缺陷，并再次进行检测和评估。期间中标人需承担由自身原因造成修改的费用。

11.2.7自系统功能检测通过之日起，采购人拥有30天的系统试运行权利。系统验收通过的日期为实际竣工日期。

11.2.8如果由于中标人原因，导致系统在试运行期间出现故障或问题，中标人应及时排除该故障或问题。以上行为产生的费用均由中标人承担。

11.2.9如果由于采购人原因，导致系统在试运行期间出现故障或问题，中标人应及时配合排除该方面的故障或问题。以上行为产生的相关费用均由采购人承担。

11.2.10系统试运行完成后，采购人应及时进行系统验收。中标人应当以书面形式向采购人递交验收通知书，采购人在收到验收通知书后的5个工作日内，确定具体日期，由双方按照本合同的规定完成系统验收。采购人有权委托第三方检测机构进行验收，对此中标人应当配合。

11.2.11 如果属于中标人原因致使系统未能通过验收，中标人应当排除故障，并自行承担相关费用，同时延长试运行期10个工作日，直至系统完全符合验收标准。

11.2.12 如果属于采购人原因致使系统未能通过验收，采购人应在合理时间内排除故障，再次进行验收。

11.2.13 采购人根据信息系统的技术规格要求和质量标准，对信息系统验收合格，签署验收意见。

**12人员及设备配备要求**

拟投入本项目的人员要求具有相关项目的实施经验，各岗位、工种配置合理，人员配置齐全，数量符合项目进度要求，主要岗位（包括项目总负责人、项目技术负责人、现场管理人员、专职安全生产管理人员）未经采购人同意不得随意更换。投标人配置项目人员的专业和数量应满足本项目的需要，专业配套齐全，委派人员需是本单位职工。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 岗位名称 | 建议配备岗位人数 | 基本要求 | 备注 |
| 1 | 项目经理 | 1 | 具备项目管理经验，善于沟通协调 |  |
| 2 | 技术负责人 | 1 | 有技术背景，熟悉相关技术或业务 |  |
| 3 | 安全管理员 | 1 | 具备安全相关经验或培训经历 |  |
| 4 | 咨询设计人员 | 2 | 具备相关项目的咨询设计经验 |  |
| 5 | 软件开发人员 | 15 | 具备相关学历 |  |
| 6 | 硬件工程师 | 2 | 具备相关学历 |  |
| 7 | 测试工程师 | 1 | 具备相关学历 |  |
| 8 | 实施部署人员 | 2 | 具备项目涉及设备安装部署、功能调试、参数配置、产品调试与实施的相关经验 |  |

**13安全生产、文明施工（安装）与环境保护要求**

13.1投标人应具备上海市或有关行业管理部门规定的在本市进行相关安装、调试服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由投标人自行负责。

13.2在项目安装、调试实施期间为确保安装作业区域及周围环境的整洁和不影响其他活动正常进行，中标人应严格执行国家与上海市有关安全文明施工（安装）管理的法律、法规和政策，积极主动加强和落实安全文明施工（安装）及环境保护等有关管理工作，并按规定承担相应的费用。中标人若违反规定野蛮施工、违章作业等原因造成的一切损失和责任由中标人承担。

13.3中标人在项目供货、安装实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

13.4中标人现场设备安装负责人应具有专业证书，安装人员必须持证上岗。中标人应对设备安装、调试期间自身和第三方安全与财产负责。

13.5中标人在组织项目实施时必须按安装施工计划协调好现场施工（安装）工作，在项目验收合格移交前对到场货物承担保管责任。中标人在项目实施期间必须保护好施工区域内的环境和原有建筑、装饰与设施，保证环境和原有建筑、装饰与设施完好。

13.6各投标人在投标文件中要结合本项目的特点和采购人上述的具体要求制定相应的安全文明施工（安装）和安全生产管理措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价措施费中列支必须的费用清单。

**14售后服务要求（包括延伸服务要求）**

**14.1 操作与维修手册**

14.1.1 技术文件：中标人提供本系统的详细技术文件

14.1.2 技术服务：

（1）投标人应有完善的技术支持与售后服务体系，根据本次招标文件所制定的目标和范围，在投标文件中提出相应的技术支持和售后服务方案。

（2）本项目需要投标人提供本地化服务，处理所有售后服务。同时可提供每周7天×24小时本地语言（中文）支持。接到采购人报修维护信息后30分钟内予以技术响应。在投标文件中详细说明售后服务方案。

（3）投标人在免费质保期内应提供每周7天×24小时本地语言（中文）支持，日常可采用远程支持的方式，通过电话、互联网提供维护服务。需每月上门巡检一至三次。

（4）投标人须做出无推诿承诺。即投标人应提供特殊措施，无论由于哪一方产生的问题而使设备发生不正常情况时，并在得到采购人通知后，需全力配合设备原厂商和其他供应商，使系统尽快恢复正常。

14.1.3 投标人应在投标文件中详细说明技术指导和技术支持的范围和程度。

**14.2 免费质保期**

14.2.1 本项目整体质量保证（免费技术支持）期为12个月，其中软件部分质保期不少于12个月，硬件部分质保期不少于36个月。质量保证期工作内容要求按照合同文件规定执行。质量保证期从项目验收通过并交付之日后起计，免费质保期内投标人应当免费提供质保服务。

14.2.2 在免费质保期内，售后服务机构或团队构成、系统发生故障后的应急响应方案；

14.2.3 如果设备发生故障，具体响应方案。中标人应调查故障原因并修复直至满足最终验收指标和性能的要求，或者更换整个或部分有缺陷的材料。以上各项都应是免费的。

**14.3 备品备件**

投标人应在投标文件中提出保修期之后的设备返修流程，包括返修时间，替用设备，以及返修价格。

**14.4 原厂售后服务承诺**

针对该项目投标人如有核心产品的原厂售后服务原厂承诺书可提供。

**15 项目的保密和知识产权**

15.1 中标人保证对其提供的服务及出售的标的物享有合法的权利，应保证在其出售的标的物上不存在任何未曾向采购人透露的担保物权，如抵押权、质押权、留置权等。

15.2采购人委托开发软件的知识产权归采购人所有。中标人向采购人交付使用的信息系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。

15.3在本合同项下的任何权利和义务不因中标人发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则中标人的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对采购人承担连带责任。

15.4 中标人应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。

15.5采购人具有源代码修改权和永久使用权。采购人对本次开发的软件拥有产权，具有软件开发平台的永久使用权，中标人在售后维护期内（包括续签的售后服务期）应提供软件开发平台的后续升级及因开发平台升级导致的应用软件升级服务。

15.6 如采购人使用该标的物构成上述侵权的，则中标人承担全部责任。

**16 技术培训**

16.1 技术文件：

中标人应提供本系统的详细技术文件，包括培训用文字资料和讲义等相关用品。

16.2 技术服务：

中标人提供对应用软件系统使用人员和管理人员的培训，培训内容包括系统的使用及维护培训。

中标人派出具有相应专业实际工作和教学经验的辅导人员进行培训。中标人采取现场培训和集中培训相结合的方式。

系统维护管理培训主要是面向系统运维人员及系统管理人员进行的培训，使其具备独立进行系统管理及日常运行维护的能力。

培训所使用的语言和教材（编制成册）应是中文，否则投标人需提供相应的翻译。投标人提供培训所需要的技术支持。

技术培训的内容需覆盖产品的安装、日常操作和管理维护，以及基本的故障诊断与排错。

四、投标报价须知

**17 投标报价依据**

17.1 投标报价计算依据包括本项目的招标文件（包括提供的附件）、招标文件答疑或修改的补充文书、工作量清单、项目现场条件等。

17.2招标文件明确的项目范围、实施内容、实施期限、质量要求、售后服务、管理要求与标准及考核要求等。

17.3工作量清单说明

17.3.1 工作量清单应与投标人须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

17.3.2采购人提供的工作量清单是依照采购需求测算出的主要工作内容，允许投标人对工作量清单内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各投标人应认真了解招标需求，如发现核心工作内容和实际采购需求不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件或补充文件予以更正，否则，应以工作量清单为准。

**18****投标报价内容**

18.1 本项目报价为全费用报价，是履行合同的最终价格，除投标需求中另有说明外，投标报价（即投标总价）应包括项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。

18.2 投标报价中投标人应考虑本项目可能存在的风险因素。投标报价应将所有工作内容考虑在内，如有漏项或缺项，均属于投标人的风险，其费用视作已分配在报价明细表内单价或总价之中。投标人应逐项计算并填写单价、合计价和总价。

18.3在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，投标人应自行考虑，在合同履约期内中标价不作调整。

18.4 投标人按照投标文件格式中所附的表式完整地填写《开标一览表》及各类投标报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

**19投标报价控制性条款**

19.1 投标报价不得超过公布的预算金额或最高限价，其中各分项报价（如有要求）均不得超过对应的预算金额或最高限价。

19.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

19.3 投标人提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。不得违反法规标准规定或合同约定，不得通过降低服务质量、减少服务内容等手段进行恶性低价竞争，扰乱正常市场秩序。

★19.4经评标委员会审定，投标报价存在下列情形之一的，该投标文件作无效标处理：

19.4.1减少工作量清单中主要工作内容数量，或设备材料参数指标中核心设备数量；

19.4.2 投标报价和技术方案明显不相符的。

五、政府采购政策

**20 节能产品政府采购**

20.1 按照《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“节能产品品目清单”中的，在技术、服务等指标同等条件下，应当优先采购节能产品。采购人需购买的材料产品属于政府强制采购节能产品品目的，投标人必须选用节能产品。

20.2投标人如选用节能产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的节能产品的认证证书；反之，该产品在评标时不被认定为节能产品。

**21环境标志产品政府采购**

21.1 按照《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“环境标志产品品目清单”中的，在性能、技术、服务等指标同等条件下，应当优先采购环境标志产品。

21.2投标人如选用环境标志产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书；反之，该产品在评标时不被认定为环境标志产品。

**22 促进中小企业发展**

**★**22.1中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业【2011】300号）执行，参加投标的中小企业应当提供《中小企业声明函》（具体格式见“投标文件格式”），反之，视作非中、小微企业，不具备参与投标资格。如项目允许联合体参与竞争的，则联合体中各方均应为中小企业，并按本款要求提供《中小企业声明函》。

**★**22.2 事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

**★**22.3 如项目允许联合体参与竞争的，组成联合体的中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

**★**22.4供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

**23** **促进残疾人就业（注：仅残疾人福利单位适用）**

23.1 符合财库【2017】141号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

23.2 残疾人福利性单位在参加政府采购活动时，应当按财库【2017】141号规定的《残疾人福利性单位声明函》（具体格式详见“投标文件格式”），并对声明的真实性负责。