**采购需求**

**前提：本章中标注“★”的条款为本项目的实质性条款，投标人不满足的，将按照无效投标处理。**

## （一）. 项目概述

1.项目概况：本项目一个包，攀枝花市生态环境局采购视频接入中心、物联网接入中心运维项目。

2.项目清单：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 包号 | 品目号 | 标的名称 | 所属行业 | 数量 |
| 01包 | 1-1 | 视频接入中心、物联网接入中心运维项目 | 软件和信息技术服务业 | 1 |

## ★（二）. 商务要求

1、服务时间：

1.1本项目运维期为2年，中标人须对用户需求及时响应，响应内容包含但不限于故障处理服务、技术咨询服务、重大活动保障、应急处置、系统运行及安全保障要求、电话热线支持、数据处理、规章制度建立,24小时内完成故障处理，3个工作日内完成安全漏洞整改。

1.2 时限要求

1.2.1技术、服务要求中视频接入中心基础环境建设、物联网接入中心基础环境建设内容要求在签订合同后1个月内完成。

1.2.2视频接入中心数据接入、视频接入中心数据对接服务、物联网接入中心数据接入、物联网接入中心数据对接服务应保证与省生态环境厅对应工作同步，原则上不超过签订合同后3个月。

1.2.3其他项目内容在运维期内完成。

2、服务地点：攀枝花市生态环境局。

3、报价要求：供应商应严格按照本项目招标文件第三章第二部分规定的开标一览表和分项报价表内容提供报价。

4、考核要求

4.1 本项目运维考核实行按月评测，按年考核。

4.2 每月开展月度评测，满分100分。

4.3 每年年末开展年度考核，年度考核得分等于全年月度评测平均分。年度考核得分≥90分视为合格。年度考核得分< 90分，视为不合格。

月度评测表

|  |  |  |  |
| --- | --- | --- | --- |
| 测评项 | 运维内容 | 分值 | 测评指标 |
| 设备巡检 | 及时发现设备或同步设备异常情况 | 10 | 未能及时发现设备异常，被上级部门发现后通报的，扣10分 |
| 视频监测 | 监测和统计监控点在线率、 图像正常率、 录像完整率、 编码设备在线率、存储设备在线率，发布近一周、近一月的监控点在线率、图像正常率数据的趋势图。 | 10 | 每月考核时未发布周、月趋势图的，扣10分 |
| 故障诊断 | 故障诊断定位分析视频丢失、 视频卡顿、 视频花屏、 数据丢失等。 | 10 | 发生故障后，不能准确定位诊断分析的，扣10分 |
| 运维工单管理 | 实现运维工单管理功能，支持派单、催单、自动催办、跟踪、结单等功能。 | 10 | 未能实现运维工单功能的，扣10分 |
| 数据资产管理 | 构建数据资产视图，掌握监控点位数据资产情况，包括监控点位基本信息、数据总量、上下架情况、位置信息、数据质量信息、数据对外服务情况、数据统计情况。 | 10 | 未能构建资产视图，或监控点位变化后未能及时更新的，扣10分 |
| 现场端NVR巡检 | 每季度对视频监控NVR现场端进行一次巡检，检查网络链路状态、NVR设备状态，并拍摄现场设备状态存档。 | 10 | 未能按时完成巡检的，扣10分 |
| 其他运维 | 系统巡检、前端设备巡检、网络质量评估、对前端设备接入故障排查、系统平台优化、软件功能升级、系统环境改变、性能评估、安全评估、安全管理、应急服务、系统管理及维护、数据管理与维护、培训服务、运维报告。 | 20 | 每发现一项没有完成的运维内容扣5分，扣完为止。每月根据运维情况提交一份运维报告，未提交本项不得分。 |
| 网络安全 | 开展网络安全等级保护测评、开展安全风险隐患排查、加强网络安全应急联动处置、网络安全事件监测能力、网络安全审计能力、终端安全防护能力、物联网安全防护能力 | 20 | 每发现一项没有完成的运维内容扣5分，扣完为止。每月根据运维情况提交一份运维报告，未提交本项不得分。 |

5、付款方式：

5.1按期完成视频接入中心数据接入、视频接入中心数据对接服务、物联网接入中心数据接入、物联网接入中心数据对接服务，实现与省生态环境厅的对接并通过采购人组织的终验后，支付合同金额的50%。如因政策性因素原因，付款时间顺延。

5.2项目运维第1年期满后（运维期自终验完成之日起开始计算），按上述第4条考核要求开展考核。结果合格的，采购人按照支付合同金额的25%。结果不合格的，则不支付当年对应的运维经费。

5.3项目运维第2年期满后，按上述第4条考核要求开展考核。结果合格的，采购人按照日常运维服务部分的50%支付对应金额。结果合格的，采购人按照支付合同金额的25%。

6、人员要求

6.1供应商为本项目配备项目经理、信息安全负责人、团队成员、驻场运维人员。

驻场运维人员要求：运维期内，中标人派遣不少于一名运维工程师在采购人办公场所驻场，接受采购人统一管理。驻场人员和采购人同步工作时间，节假日按国家假日办规定执行。驻场人员负责现场的运维服务和支持，包括硬件设备安装和维护、软件配置和调试、故障排除和处理、用户培训和支持等。驻场运维人员全部费用由中标人承担。驻场运维人员需自带计算机。中途更换驻场运维人员需经采购人同意，且更换的驻场人员与原有人员具有相同技术水平，持有相同或更高级别职业资格证书。

6.2中标供应商所提供的服务质量须达到采购人的要求，在保证服务期和服务质量的前提下为采购人提供服务，服务中的一切风险（包括人员安全事故责任、与第三方的劳务纠纷、项目实施过程中的劳务纠纷及人员伤害等）均由中标供应商一方承担责任。

7、培训：2年内提供不低于2次的集中技术培训（含区县）。

8、本地化保障：中标人在运维期内应提供相应的车辆、技术人员 ，协助采购人对本项目涉及的前端视频和物联网设备每季度开展巡检工作，季度巡检量不低于所有设备的25%，全年巡检量不低于所有设备的90%（考虑对部分故障率高的设备加大巡检频率，运行良好设备减少巡检频率的情况）。巡检量未达标的则当年考核直接视为不合格。

9、履约验收标准：

9.1验收程序：如出现未在采购文件中明确规定的，以国家或行业相关标准为准。如采购双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在采购文件与投标文件中按质量要求和技术指标、行业标准比较优胜的原则确定该项的约定标准进行验收。如出现争议，在场验收人员无法确定的，委托第三方质检机构进行检测，检测费用由中标人垫付，最终验收标准以检测结果为准，如检测合格由采购人承担检测费用，如检测不合格由中标人承担。验收的主要依据如下:（1）国家相关的法律法规；（2）国家或行业相关标准规范；（3） 本项目招标文件、投标文件；（4）项目合同及其附件；（5）其他相关文件资料。其他未尽事项按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库[2016]205号）文件的规定要求及国家行业主管部门规定的标准、方法和内容进行验收。

9.2验收主体：攀枝花市生态环境局。

9.3验收方式：供应商提出验收申请之日起 7日内组织验收。

10、知识产权归属和处理方式：

10.1供应商应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。

10.2采购人享有本项目实施过程中产生的知识成果及知识产权。

10.3如采用供应商所不拥有的知识产权，则在报价中必须包括合法获取该知识产权的相关费用。

11、成本补偿和风险分担约定：

11.1在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

11.2不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

11.3不可抗力事件延续20天以上，双方应通过友好协商，确定是否继续履行合同。

12、技术履约验收内容：按国家有关规定以及采购人招标文件的质量要求和技术指标、供应商的投标文件及承诺与本项目合同约定标准进行验收

13、商务履约验收内容：严格按照招标文件要求及投标文件应答进行验收。

## ★（三）. 技术、服务要求

|  |  |
| --- | --- |
| 项目名称 | 技术要求 |
| 视频接入中心基础环境建设 | 中标人完成软件基础环境准备、软件部署调试。具体内容包括但不限于如下：  1.中标人提供银河麒麟服务器操作系统V10 SP2或以上版本一套，提供人大金仓数据库一套，用于物联网接入中心部署（本项目共需提供两套服务器操作系统和数据库，分别用于视频接入中心和物联网接入中心）。  2.操作系统安装。在已有的H3C CAS7.0云平台中安装银河麒麟操作系统，并完成操作系统基本配置如计算机名1、时区2、NTP3、配置用户帐户4、配置网络5、安装ssh6、路由跟踪7、必要的软件8（如：文本编辑器、压缩软件、网络调试工具）等；完成操作系统安全基线防护配置，如防火墙管理9、危险端口禁止10、安装杀毒软件11、系统日志配置12、密码策略13、登录策略14。  3.数据库安装和部署。安装人大金仓数据库，完成数据库密码策略配置15、配置用户权限16、配置数据库备份策略17、开启数据库审计和日志记录18等。  4.视频接入平台软件部署。完成平台软件部署，记录安装过程、所使用的中间件、所使用的计算机端口、应用软件存放地址、数据库存放地址、备份存放地址、平台访问地址。完成平台用户管理、平台基础资料录入等。  5.网络边界安全防护能力：为已有的网络边界安全防护设备，购买2年的官方厂家质保，质保内容应包括软硬件维护及补丁、特征库、病毒库的更新服务等，具体要求见“网络边界安全防护设备质保要求”表。  6.接入130个NVR（海康、大华），最终接入数以实际情况为准。  7.现场端NVR升级改造：对于单网口的现场端进行改造，中标人提供50台路由设备（每台配置至少1个WAN口，4个LAN口），路由设备连接视频专网和NVR本地网，启用NAT转换和端口映射功能，隐藏内网摄像机和NVR地址。  8.改造4台大疆无人机，实现数据实时回传功能，包含2年网络通讯费用。  9.改造10台单兵执法记录仪（警翼），实现现场执法视频实时回传功能，包含2年的网络通讯费用。  10.改造6个马店河视频监控点位，实现各监测点位太阳能电池板和电力线双源供电，现场视频实时回传。包含2年网络通讯费用。  注：以上内容涉及的技术资料在项目验收时提供详细纸质文档。 |
| 视频接入中心数据接入 | 视频数据接入实现各级生态环境部门视频监控设备及各类环保监管企业的IPC（网络摄像机）、DVR（数字硬盘录像机）和NVR（网络录像机）等数字视频编码设备和存储设备接入市（州）视频接入平台。视频接入平台通过国标GB/T 28181进行上下级域的方式进行互联对接省统一视频接入平台，功能满足包括GB/T28181协议中规定的注册、实时视音频点播、设备控制、设备信息查询、状态信息报送、历史视音频文件检索、历史视音频回放、历史视音频文件下载、网络校时、订阅和通知等。 |
| 视频接入中心运维管理 | 中标人提供软件平台运维管理服务，运维包括备设备巡检、视频监测、故障诊断以及运维工单管理、数据资产管理功能。  1.设备巡检：及时发现设备或同步设备异常情况；  2.视频监测：监测和统计监控点在线率、 图像正常率、 录像完整率、 编码设备在线率、存储设备在线率，发布近一周、近一月的监控点在线率、图像正常率数据的趋势图。  3.故障诊断：故障诊断定位分析视频丢失、视频卡顿、视频花屏、数据丢失等。  4.运维工单管理：实现运维工单管理功能，支持派单、催单、自动催办、跟踪、结单等功能。  5.数据资产管理：构建数据资产视图，掌握监控点位数据资产情况，包括监控点位基本信息、数据总量、上下架情况、位置信息、数据质量信息、数据对外服务情况、数据统计情况。  6.现场端NVR巡检：每季度对视频监控NVR现场端进行一次巡检，检查网络链路状态、NVR设备状态，并拍摄现场设备状态存档。 |
| 视频接入中心数据对接服务 | 生态环境业务应用的整合共享对接包括了与省厅视频中心、中台、4A等多个系统以及本项目相关平台的对接。  1.与省厅视频中心对接服务：市局视频接入中心实现与省级平台的对接，实现省级平台对攀枝花市视频数据的实时调用能力，包括视频统一接入中心的音视频处理、设备控制管理、故障诊断等能力；获取市（州）级视频统一接入中心已部署监控点位的实时视频数据及相关点位信息;实时获取市（州）级视频统一接入中心视频报警数据信息等。  2.与市级业务系统对接服务：市局视频接入中心实现市内的系统和设备的对接工作和视频数据的实时调用能力，中标人需提供对接服务。  3. 4A认证服务：市局视频接入平台可与省厅基础支撑4A系统的统一安全认证与统一身份管理进行集成，用户管理模块需要实现用户权限信息修改、分组管理、有效期管理等功能。市局视频接入平台可与省厅基础支撑4A系统的统一授权进行集成，各个模块都需要按照用户、用户组进行权限区分与管理，使不同的用户、用户组查看使用不同的模块与内容。  5.GIS地理信息服务：视频接入中心实现与市局地理信息服务进行对接，获取地理信息和各类环境要素的展示能力。  6.与技术支撑层能力系统及上层业务应用系统对接服务：通过与技术支撑层智能系统的对接。如，将视频数据信息提供给智能语音、图像识别技术系统，构建生态环境智能化管理能力；提供给以人脸识别、烟雾识别、水污染识别、语音识别技术系统，构建污染监控视频智能分析能力；提供给智能语音、智能识别系统，实现构建智能监控的支撑能力。并将这些能力通过接口提供给上层业务应用系统。 |
| 物联网接入中心基础环境建设 | 中标人完成软件基础环境准备、软件部署调试。具体内容包括但不限于如下：  1.中标人提供银河麒麟服务器操作系统V10 SP2或以上版本一套，提供人大金仓数据库一套，用于物联网接入中心部署（本项目共需提供两套服务器操作系统和数据库，分别用于视频接入中心和物联网接入中心）。  2.操作系统安装。在已有的H3C CAS7.0云平台中安装银河麒麟操作系统，并完成操作系统基本配置如计算机名、时区、NTP、配置用户帐户、配置网络、安装ssh、路由跟踪、必要的软件（如：文本编辑器、压缩软件、网络调试工具）等；完成操作系统安全基线防护配置，如防火墙管理、危险端口禁止、安装杀毒软件、系统日志配置、密码策略、登录策略。  3.数据库安装和部署。安装人大金仓数据库，完成数据库密码策略配置、配置用户权限、配置数据库备份策略、开启数据库审计和日志记录等。  4.物联网接入平台软件部署。完成平台软件部署，记录安装过程、所使用的中间件、所使用的计算机端口、应用软件存放地址、数据库存放地址、备份存放地址、平台访问地址。完成平台用户管理、平台基础资料录入等。  以上技术资料在项目验收时提供详细纸质文档。 |
| 物联网接入中心数据接入 | 物联网接入中心汇聚攀枝花市生态环境局业务科室物联网数据、业务系统数据。包括但不限于：重点污染源在线自动监测系统、机动车尾气遥感管理系统、水污染溯源精细化监管系统、空气质量微站监测系统、固定污染源智能监管平台等。 |
| 现场端接入服务 | 提供接入符合技术标准的多种品牌型号前端设备的能力。提供前端设备接入调试服务，包括公开对HJ 212-2017协议扩展的字段，为前端设备分配编号、设备接入成功判断、接入失败原因分析，帮助企业接入平台。 |
| 运维管理 | 同“视频接入中心运维管理”技术要求。 |
| 物联网接入中心数据对接服务 | 同“视频接入中心数据对接服务”技术要求。 |
| 其他运维要求 | 1.系统巡检：对本次项目建设的各个业务系统进行系统巡检，查看平台软件服务是否启用、链接是否可用、操作系统CPU、内存是否正常、硬盘是否有足够的空间，并对关键数据、程序及日志进行备份，防止数据丢失，并记录到巡检报告。  2.前端设备巡检：对前端数据采集设备（包括视频摄像头、硬盘录像机、无人机、移动执法记录仪、单兵设备、数采仪等）连接以及运行状况进行定期远程巡检，发现设备离线、故障等情况通知设备运维人员，并记录到巡检报告。  3.网络质量评估：采用运行自定义脚本评估网络服务质量，并提供分析报告及进一步改进措施和建议。评估和优化指标如下：网络结构、网络吞吐量、网络流量、网络延迟。  4.对前端设备接入故障排查:对调试失败的设备给出明确的故障原因和指导解决方案。要求帮助所有需要接入的企业完成接入，提供排障、指导服务，无任何理由拒绝企业的接入。  5.系统平台优化：配合省厅完成系统负载能力优化、用户界面优化、平台系统兼容性优化。  6.软件功能升级：有新版本时，配合完成系统升级，并提交升级后新版本介质、升级技术文档、用户手册、管理手册等。  7.系统环境改变：当承载系统运行的基础环境改变，如硬件、系统软件版本升级、补丁更新，运维工程师完成相应系统的升级工作，并与应用系统进行集成测试，确保系统在新环境下运行稳定。  8.性能评估：定期采用工具评估系统的性能，并提供分析报告及进一步改进措施和建议，评估和优化的范围包括网络设备、应用系统等。评估和优化的指标如下：响应时间、吞吐量、资源使用率、并发用户数。  9.安全评估：定期从数据安全、网络安全、物理安全、主机安全等方面对系统平台的运行环境进行评估。  10.安全管理：系统所处基础硬件环境的网络安全设备管理及升级维护；网络安全设备的运行管理，主要包括访问策略的制定、修改、配置更改等维护，安全级别的设定和调整，安全日志保护；信息安全管理，对于不同共享平台中产生的大量信息，按照其重要性或保密性要求，进行信息分级，并采取不同的数据备份措施和数据恢复措施。  11.应急服务：对系统运行过程中可能出现的以下几类突发性问题——系统瘫痪、设备损坏、线路故障、系统错误、操作失误、病毒破坏及非法入侵，提供相应的紧急情况技术支持。  12.系统管理及维护：维护系统的稳定运行，包括运行环境、数据库系统、平台等的配置、运行维护、故障检测、升级、恢复等。  13.数据管理与维护：系统平台数据库备份、APP数据备份、设备及系统主要配置文件备份、备份数据的有效性检查等；按可行数据恢复计划对关键数据进行恢复。  14.培训服务：根据项目涉及的系统使用说明书和系统维护说明书等内容，需要对运行管理人员、终端用户等工作人员采取灵活的方式进行培训。  15.运维报告：按时规范提交运维周报、运维月报、故障记录、半年总结报告和年度报告等运维资料。 |
| 网络安全要求 | 1.开展网络安全等级保护测评：按照省厅要求，开展网络安全等级保护定级备案和等保测评工作，出具测评报告。  2.开展安全风险隐患排查：每月对系统至少开展一次安全漏洞扫描并出具扫描报告，并于7日内完成漏洞修复，形成漏洞处置记录。每年通过渗透测试、基线核查、风险评估等方式开展网络安全风险隐患排查，出具报告，并及时整改处置。每月至少开展一次系统账户、口令使用情况的检查，杜绝弱口令。  3.加强网络安全应急联动处置：制定应急预案，提供人员和技术支持，确保运维期内采购人顺利通过省生态环境厅、市公安局、市网信办等主管部门组织的应急演练。  4.网络安全事件监测能力：对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。监测到的网络安全日志应实现与省厅共享。  5.网络安全审计能力：提供全面收集存储审计安全设备、网络设备、数据库、服务器、应用系统、主机等设备日志（包括运行、告警、操作、消息、状态等）的能力。提供监控和记录运维人员对服务器、网络设备、安全设备、数据库等设备操作行为的能力。  6.终端安全防护能力：具有终端网络安全管控能力，能对终端非法内联、违规外联、软件安装、进程运行等行为进行管控，能保障计算机、服务器等终端设备的安全运行，能实现对用户终端的统一安全管控，定期统一下发补丁、病毒查杀。  7.物联网安全防护能力：具有对物联网资产（包括但不限于录像机、视频摄像头等）流量监控、资产画像、资产管控、基线异常行为告警、资产仿冒控制、资产入网审批、隔离控制、访问控制、异常监测等安全防护的能力。 |

网络边界安全防护设备质保要求

|  |  |  |  |
| --- | --- | --- | --- |
| 设备名称 | 设备型号 | 设备数量 | 服务内容 |
| 上网行为管理器 | AC-1000-E620 | 1 | URL&应用识别规则库升级（两年）  产品质保（两年）  软件升级（两年） |
| 上网行为管理器 | AC-1000-E620 | 1 | URL&应用识别规则库升级（两年）  产品质保（两年）  软件升级（两年） |
| 上网行为管理器 | AC-1000-E620 | 1 | URL&应用识别规则库升级（两年）  产品质保（两年）  软件升级（两年） |
| 防火墙 | AF-1000-E420 | 1 | 深信服云智订阅软件（两年）  产品质保（两年）  软件升级（两年） |
| WAF | WAF-1000-DA00 | 1 | 深信服云智订阅软件（两年）  产品质保（两年）  软件升级（两年） |
| VPN | VPN-1000-C600 | 1 | 产品质保（两年）  软件升级（两年） |
| 安全态势感知 | SIP-1000-E600 | 1 | 软件升级（两年） |
| 日志审计系统 | LAS-1000-C600 | 1 | 产品质保（两年） |
| 基线核查系统 | BVT-1000-C640 | 1 | 产品质保（两年）  软件升级（两年） |
| 数据库审计 | LA-DAP-1600-UR | 1 | 硬件设备两年的维保服务；  5×8技术支持服务。 |
| 入侵防御 | Power V6000-P3320 | 1 | 硬件设备两年的维保服务；  5×8技术支持服务；  防病毒两年升级费用；  入侵防御系统特征库两年升级服务； |
| 入侵防御 | Power V6000-P3320 | 1 | 硬件设备两年的维保服务；  5×8技术支持服务；  入侵防御系统特征库两年升级服务； |
| 防火墙 | Power V6000-P3320 | 1 | 硬件设备两年的维保服务；  5×8技术支持服务。 |
| 堡垒机 | OSM-4600 | 1 | 硬件维修服务（两年）；  同代软件版本升级服务（两年）；  5×8热线技术支持服务。 |