第三章 招标项目技术、服务、商务及其他要求

（注：当采购包的评标方法为综合评分法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

（注：当采购包的评标方法为最低评标价法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1采购项目概况

（1）朱鹮监测系统提升：鸟类智能识别软件平台1项。（2）配套中心机房提升：AI识别服务器2台。（3）信息安全：下一代防火墙1台，日志审计1台，杀毒软件1套，等保测评1项。

3.2采购内容

采购包1：

采购包预算金额（元）: 640,000.00

采购包最高限价（元）: 640,000.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否核心产品	是否允许进口产品	是否属于节能产品	是否属于环境标志产品
1	鸟类智能识别系统(含配套设备)	1.00	640,000.00	套	软件和信息技术服务业	否	否	否	否

3.3技术要求

采购包1：

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

标的名称：鸟类智能识别系统(含配套设备)

<table>
<tr><th>参数性质</th><th>序号</th><th>技术参数与性能指标</th></tr>
<tr><td></td><td></td><td>系统软件及硬件的技术参数要求：
<table>
<tr><th>序号</th><th>产品（服务）名称</th><th>具体技术（服务）参数要求</th><th>数量</th><th>单位</th><th>备注</th></tr>
<tr><td></td><td></td><td>（1）首页主要包括精美素材、珍稀提示、设备告警、监测设备分布图、珍稀提示统计、物种遇见频次占比、种群栖息趋势、定点监测结果、鉴定通知等模块。内容包括鸟类监测</td><td></td><td></td><td></td></tr>
</table></td></tr>
</table>

				过程中各类监测、识别数据，展示一个直观的、总体的监测结果，方便用户整体把握保护区鸟类资源现状。 （2）能够对鸟类进行实时监测，能够及时掌握保护区内鸟类种类、数量情况，包括周期巡航 、定制抓拍、特定追踪、关怀识别等模块。具有实时识别相关证明材料。 （3）包括历史周期巡航记录、历史定制抓拍记录、历史特定追踪记录、历史关怀识别记录、告警记录、提示记录等模块。通过历史监测数据，实现对鸟类出现时段、地点的监测，以及鸟类种类趋势的分析，科学展示候鸟的习性和迁徙规律，反映保护区生态环境变化状况，为探究保护区小气候变化与鸟类栖息、迁徙间的关系提供平台与依据，为保护区管理、评价、科学研究等提供精准的参考和强有力的技术支撑。 （4）支持鸟类监测鉴定，对收集的鸟类图像进行人工识别鉴定，并支持进行标注和图像分类。鸟类相册按日期进行分类，每张图像显示已鉴定或未鉴定状态，对漏识别图像支持人工识别，并进行标注，对识别错误图像支持修改，识别结果包括监测时间、照片编号、监测设备、照片质量、物种名称，可				
			1	鸟类智能识别软件平台		1	项		

				对图像进行标注。 （5）支持统计分析，根据监测的鸟类物种及数量，计算当月或当年的鸟类多样性指数，并统计当年的鸟类多样性趋势。展示内容包括鸟类多样性指数、鸟类多样性趋势图、设备监测种类统计、设备监测数据统计、设备采集素材数量统计、珍稀物种占比、珍稀物种监测趋势、综合物种遇见频次、综合物种热力分布对比、珍稀物种热力分布对比、居留类型统计，所有统计数据均可通过时间筛选。 （6）支持物种名录，对收集的鸟类数据进行整理，形成物种库，展示界面包括物种库以及所选物种的详细信息。物种库展示界面包括物种图片、物种名称、添加时间、保护等级、识别等级；物种详细信息包括物种名称、类别、形态特征、栖息环境、生活习性、分布范围、繁育方式、保护现状、人工饲养信息；物种库和物种详细信息均支持添加、删除、修改功能模块。具有鸟类数据监测相关证明材料。 （7）具有按周、月、年数据分析汇总，自动生成报告，数据导出Excel表格功能。			

		2	AI识别服务器	（1）CPU:2*4310，12核24线程; （2）磁盘阵列卡:R730-8I; （3）内存:≥128G; （4）硬盘:≥3*2.4T，企业级硬盘; （5）GPU:≥2070; （6）电源:≥800W*2; （7）系统:≥UBUNTU 20.04。	2	台	
				性能参数：网络层吞吐量≥4G，应用层吞吐量≥1G，并发连接数≥100万，HTTP新建连接数≥2.5万。1U机架式设备，内存大小≥4G，硬盘容量≥128G SSD，接口≥8千兆电口+2千兆光口SFP。 1.产品支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。 2.产品支持策略路由负载，支持基于服务、ISP地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。 3.产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 4.产品支持支持源地址转换SNAT，目的地址转换DNAT和双向NAT等功能，支持一对一、一对多、多对一等形式的NAT。			

		3	下一代防火墙	5.产品支持云情报网关技术，通过全球超过30+pop节点，实现对威胁流量进行实时检测&拦截，所有流量在转发前均经过威胁情报的检测并已明确结果，实现恶意流量在转发前被阻断，保护资产安全。（提供第三方官方机构针对上述功能的检测证书和POP节点在线查询网站） 6.产品支持对HTTPS协议加密流量进行解密，支持配置基于区域、对象、业务类型、服务器IP/端口的解密策略。 7.产品支持对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置。 8.支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息（提供相关功能截图并加盖厂商公章）。 9.产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。 10.产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。	1	台		
				性能参数：2U标准机架设				

	1				备，≥16G内存，≥6个千兆电口；≥4T硬盘；≥1个console口，≥2个usb接口，日志处理速率≥2500 EPS。 1.提供安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于720种日志对象的日志数据采集能力； 2.提供主动、被动相结合的数据采集方式的能力，支持通过Agent采集日志数据;支持syslog，sftp，jdbc，snmp trap标准日志接口；支持文件夹采集，支持文件通配符过滤采集； 3.提供通过正则、分隔符、json、xml的可视方式进行自定义规则解析的能力，支持对解析结果字段的新增、合并、映射； 4.提供对每个日志源设置过滤条件规则的能力，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用； 5.提供对单个/多个日志源批量转发的能力，支持转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志； 6.提供TLS加密方式进行日志传输能力，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输				

		4	日志审计	总量； 7.提供以FTP方式将日志数据备份至外部存储空间的能力，支持备份数据的恢复和查询；支持自动备份归档方式。 8.提供通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索能力；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；（提供相关功能截图并加盖厂商公章）。 9.提供解码小工具能力，可以按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等； 10.提供网站攻击、漏洞利用、C&C通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则的能力，内置关联分析规则数量达到350条以上，支持自定义关联分析规则； 11.具备同类告警合并策略，减少告警数量； 12.提供管理员账号创建、修改、删除能力，并可针	1	台		

				对创建的管理员进行权限设置；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求； 13.提供个性化定制能力，支持全系统更换logo与系统名称，支持一键恢复默认；				
				1.单一管理控制中心可统一管理分别部署在Windows服务器、Linux服务器以及国产化服务器的客户端软件； 2.支持对Windows终端的漏洞情况进行扫描，并查看漏洞具体情况及KB号，并显示具体修复情况；支持对流行Windows高危漏洞的轻补丁免疫防御。（提供相关功能截图，并加盖厂商公章） 3.支持全网视角的主机资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户；支持对单个终端主机运行状态的监控，包括但不限于进程、服务、网络连接、计划任务和开放共享信息 4.具备针对最新未知的文件，使用IOC特征（文件hash、dns、url、ip等）的技术，进行检测。 5.支持一键云鉴定服务，提供云端专家+沙箱+多引擎鉴定能力，结合云端威胁情报对已告警的威胁				

		5	杀毒软件	文件再次进行综合研判，用户可自助对管理平台告警的威胁快速判断是否误报和了解威胁详情。 6.构建全网文件信誉库，当一台终端发现某一病毒文件，全网可进行感知并进行针对性查杀，支持处置病毒时选择是否在其它主机上同步处置。 7.支持禁止黑客工具启动，包含：冰刃、xuetr、ProcessHacker、PCHunter、火绒剑、Mimikatz的自启动，可以防止黑客攻击。 8.支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截；支持对勒索入侵的主流方式RDP暴破做全方位保护，包括RDP登录校验、RDP文件加白二次校验等功能（提供相关功能截图，并加盖厂商公章） 9.一键式操作对指定Windows终端/终端组进行合规性检查，包括身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范，对不合规的检查项提供设置建议，并可视化展示基线合规检查结果。 10.支持图形化显示业务系统、服务器及流量详情；流量线详情支持展示该流量线对应的控制策略；图形化显示服务器间流量关	1	套			

				系，包括访问详情、流量趋势等。 11.采用B/S架构的管理控制中心，具备安全可视，统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能 12.与此次投标的全网行为管理和下一代防火墙设备进行联动，自动化进行事件的处置和关联分析的举证等（提供相关功能截图，并加盖厂商公章）				
		6	等保测评	二级等保测评	1	项			

3.4商务要求

3.4.1交货时间

采购包1：

合同履行期限（供货期限）：2024年12月20日前完成所有项目内容。

3.4.2交货地点

采购包1：

陕西汉中朱鹮国家级自然保护区

3.4.3支付方式

采购包1：

分期付款

3.4.4支付约定

采购包1： 付款条件说明： 合同签订后，达到付款条件起 5 日内，支付合同总金额的 30.00%。

采购包1： 付款条件说明： 硬件设备到货后，达到付款条件起 5 日内，支付合同总金额的 40.00%。

采购包1： 付款条件说明： 项目竣工之日起，达到付款条件起 5 日内，支付合同总金额的 30.00%。

3.4.5验收标准和方法

采购包1：

符合质量验收标准要求

3.4.6包装方式及运输

采购包1：

涉及的商品包装和快递包装，均应符合《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）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

3.4.7质量保修范围和保修期

采购包1：

合同内所有产品，保修期1年

3.4.8违约责任与解决争议的方法

采购包1：

按照合同约定执行

3.5其他要求

无