AI警务智能体建设、打击网络赌博及网赌涉案关系网络分析系统建设项目采购需求

一、基本要求

1.项目概况：AI警务智能体建设、打击网络赌博及网赌涉案关系网络分析系统建设项目，主要内容为：

合同包1（AI警务智能体建设）：AI警务智能体服务器搭建,专用软件开发等。

合同包2（打击网络赌博及网赌涉案关系网络分析系统建设）：建设搭建打击网络赌博及网赌涉案关系网络分析系统服务器，开发专业软件等。

2.预算资金：8,197,142.00元。

3.合同履行期限：合同签订生效且具备实施条件之日起60日历天内完成系统建设上线、调试完毕。

4.项目实施地点：白水县城五马路公安局。

5.采购方式：公开招标。

6.是否专门面向中小企业采购：合同包1非专门面向中小企业采购，合同包2专门面向小微企业采购。

7.采购项目需要落实的政府采购政策：①《财政部国家发展改革委关于印发〈节能产品政府采购实施意见〉的通知》（财库〔2004〕185号）；②《财政部环保总局关于环境标志产品政府采购实施的意见》（财库〔2006〕90号）；③《国务院办公厅关于建立政府强制采购节能产品制度的通知》（国办发〔2007〕51号）；④《财政部司法部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）；⑤《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库〔2016〕125号）；⑥《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）；⑦《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）；⑧《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）；⑨《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）；⑩《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15号）；⑪《关于运用政府采购政策支持乡村产业振兴的通知》（财库〔2021〕19号）；⑫《财政部农业农村部国家乡村振兴局中华全国供销合作总社关于印发<关于深入开展政府采购脱贫地区

农副产品工作推进乡村产业振兴的实施意见>的通知》（财库〔2021〕20 号）；⑬《陕西省财政厅关于进一步加强政府绿色采购有关问题的通知》陕财办采〔2021〕29 号；⑭《财政部关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19 号）；⑮《陕西省财政厅关于进一步加大政府采购支持中小企业力度的通知》（陕财办采〔2022〕5 号）；⑯《陕西省财政厅关于落实政府采购支持中小企业政策有关事项的通知》（陕财办采函〔2022〕10 号）；⑰财政部生态环境部工业和信息化部关于印发《绿色数据中心政府采购需求标准（试行）》的通知（财库〔2023〕7 号）；⑱如有最新颁布的政府采购政策，按最新的文件执行。

二、需执行的国家相关标准、行业标准、地方标准或者其他标准、规范标准

本项目所涉及的软硬件产品、系统建设及服务，必须符合但不限于以下中华人民共和国现行有效的强制性国家标准、行业标准、地方标准以及其他相关的规范性文件。如标准间存在不一致，应以最新发布或更严格的标准为准。若未明确提及，供应商应在其投标文件中明确其所依据的标准体系。

《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）；

《信息技术软件产品评价质量特性及其使用指南》（GB/T16260-2006）；

其他与本项目相关的软件工程、硬件设备、数据接口、安全保密等技术标准与规范。

三、采购标的具体要求：

（一）合同包 1（AI 警务智能体建设）

1.软件部分

序号	模块	功能项	二级功能	功能描述	单位	数量
1	法律法规关联搜索	法律法规数据整合与结构化	法律文本结构化处理	为了确保法律条文能够被快速准确地检索和关联，需要对法律文本进行结构化处理。数据结构化包括对法律条文、解释、司法案例等信息进行标准化存储，采用格式如 JSON、XML 或关系型数据库存储数据。	项	1
2			法律文本语义标注	为了提高检索效率，还需要进行语义标注，包括但不限于条文编号、法律条文的适用范围、关键词、关联条文等。	项	1
3		法律文本的语义理解与匹配	语义分析	采用语义理解与匹配技术，从案件描述中提取出相关的法律要素，并通过语义分析与法律条文之间的匹配，实现案件与法律条文的精准关联。利用自然语言处理（NLP）技术，对案件内容和法律条文进行语义分析、句法分析和依赖分析等，从而实现案件描述与法律条文的精准匹配。	项	1
4			实体识别	进行命名实体识别（NER），识别案件描述中的人物、地点、时间、案件类型等关键实体。	项	1
5			向量化处理	实现语义匹配与向量化，识别上下文信息，将案件描述与法律条文通过文本向量化技术转化为数值向量表示，计算其相似度。	项	1

6			图谱化展示	法律文本知识图谱展示，通过构建法律领域的知识图谱，将不同法律条文之间的关系可视化，以增强匹配效果。	项	1
7		法律法规排序与主次提示	条文优先级排序	实现条文优先级排序。根据案件类型为法律条文分配优先级，并按照优先级对法律条文进行排序。对于案件中的关键点，智能体自动标记，突出显示其在案件中的重要性。	项	1
8			时间排序与时效性分析	根据案件的发生时间，优先推荐相关法律条文的最新版本，同时能够处理法律修订前后的差异。	项	1
9		智能标注与关键提示	关键词高亮	关键词高亮显示。自动高亮显示与案件关键词相关的部分，方便快速定位条文中的关键内容。	项	1
10			法律条文注释	法律条文注释。部分法律条文内容较为复杂，提供简明的法律解释或注释，帮助警务人员更好地理解条文内涵。	项	1
11			风险提示与警示	风险提示与警示。在法律条文检索结果中，针对案件的特殊性，提供潜在的法律风险提示，如特定罪名的量刑标准、诉讼时效的限制等，以避免在案件处理中出现法律适用上的遗漏或错误。	项	1
12	办案流程指引	案件受理引导	案件信息登记	进行案件信息登记，指导警务人员填写案件登记表，确保关键信息（如案件来源、当事人信息等）不会遗漏。	项	1
13			受理流程提示	进行受理流程提示，提供案件受理的详细流程，引导警务人员逐步完成。	项	1
14		立案调查引导	辅助调查方案制定	辅助调查方案制定，根据案件性质，提供相关调查方法的推荐，如询问证人、勘察现场等。	项	1
15			调查进度追踪	进行调查进度追踪，记录案件调查的进展，确保所有必要的调查环节得到妥善处理。	项	1
16		审查起诉引导	材料清单及法律条文提示	辅助起诉材料准备，引导警务人员准备起诉所需相关材料，并提供清单化操作。进行法律条文提示，根据案件性质提供相关的法律条文和司法解释，确保起诉材料符合相关法律法规。	项	1
17			法律条文提示	根据案件性质提供相关的法律条文和司法解释，确保起诉材料符合相关法律法规。	项	1
18		审判与执行引导	录入信息生成报告	进行审批执行引导，根据录入信息生成相应的报告，辅助案件结案的执行与归档。	项	1
19			提交涉案证据生成报告	进行审批执行引导，根据提交的涉案证据生成相应的报告，辅助案件结案的执行与归档。	项	1
20	同类案例参考	同类案例参考	相似案件提取	为警务人员提供快速、精准的案件参考服务。通过输入案件的基本信息（如案件类型、案情要素、涉及的法律条文等），进行相似度计算与匹配，基于提取出的案件要素，通过相似度计算算法对历史数据库中的案件进行比对。根据案件各要素的权重，计算当前案件与历史案件之间的相似度，并选择与当前案件最为相似的若干个案件进行推荐。	项	1
21			多维度要素提取	在初步推荐结果基础上，智能体进一步进行多维度筛选，优化推荐结果。实现从历史案件数据库中检索出与当前案件相似的案例，并提供相关的处理建议、裁判意见和法律依据，帮助警务人员在案件办理过程中获得有价值的参考数据，以提高案件处理的质量和效率。	项	1
22	侦查手段索引	案件类型与侦察手段的关联	案件类型快速检索	进行案件分类选择，根据案件性质提供分类选项。	项	1
23			侦察手段关联	提供根据案件类型快速检索所需侦查手段的功能，方便警务人员在遇到特定案件时能够一目了然地获得相关侦查手段的指导。关联侦查手段，根据案件类型展示与之相关的侦查手段。	项	1
24		侦查手段的详细说明与应用	手段描述及局限性、风险分析	详细描述每种侦查手段的基本原理和应用场景，并进行局限性和风险分析。支持根据案件的性质，描述该侦查手段的具体应用场景。支持详细描述这些局限性和潜在的风险点，帮助警务人员判断是否适合在当前案件中使用该手段。	项	1

25		指导	操作步骤说明	操作步骤说明。提供实施每种侦查手段的具体操作步骤，必要时可以附带案例或视频教程。支持列出每种侦查手段的操作步骤，并对某些可能的操作风险、常见错误或注意事项进行提醒。	项	1
26			法律法规参考	法律法规参考。提醒使用侦查手段时需遵循的法律规定，确保操作合法合规。支持嵌入合规性检查，提醒警务人员在使用侦查手段时遵循合法程序。如在进行物证勘查时，智能体可以提醒是否符合搜查程序等。针对某些侦查手段，提醒需要遵守的相关隐私保护法律，帮助警务人员了解和遵守相关的隐私保护规定。除了列出相关法律规定，还可以提醒警务人员违反相关法律或程序可能面临的法律责任。通过警示和提示，提醒警务人员保持高度警觉。	项	1
27		智能检索与推荐	关键词匹配	根据案件特征和历史数据进行智能推荐。根据输入的案件关键词、案件特征等信息，自动推荐相关的侦查手段。关键词匹配。通过分析案件描述中的关键词，自动匹配出相关的侦查手段。	项	1
28			历史案例对比	历史案例对比。根据过往类似案件的经验，推荐相应的侦查手段。	项	1
29		侦查手段的动态更新与优化	动态更新	提供侦查手段的动态更新与优化。对新的侦查技术或方法及时纳入，确保警务人员在实际工作中能够使用到最新的侦查手段。定期更新侦查手段库，增加新的侦查工具或方法。	项	1
30			技术优化	当出现新的侦查技术时，能推送相关的培训和操作指南。	项	1
31		案例分析与参考	案件库查询	提供并总结归纳历史案件中成功运用某种侦查手段的实例，根据侦查手段或相关案件类型查找历史成功案例，供警务人员参考。通过分析这些案例，警务人员可以更好地理解侦查手段的实际效果和适用条件，从而提升侦查工作的效率与准确性。	项	1
32			案例总结与经验分享	对每个案例提供总结，列出成功的侦查策略与关键点。	项	1
33	调证数据比对分析	调证数据处理	调证数据比对条件设置	通过精确数据匹配算法对各类型数据按条件比对分析。支持调证反馈的各类型数据（word/excel/pdf/txt 等）按各类条件进行比对操作。根据具体需求设置比对分析条件，如按时间区间、地理位置、人物属性、案件类型、关键字、金额等。	项	1
34			地理位置数据处理	地理位置数据可以通过地理编码技术进行比对。	项	1
35			文本数据处理	文本数据可以利用自然语言处理技术进行模糊匹配。	项	1
36			时间数据处理	时间数据则需通过时间戳对比来分析其关联性。	项	1
37		数据可视化展示	交互式分析界面	提供交互式分析界面，支持比对结果可视化，支持数据动态更新与及时反馈。可视化展示不仅具备静态的图表，还具备交互式的功能，根据需求调整视图、缩放区域、筛选条件等。支持在地图上缩放查看某一地区内的案件分布，或者点击图表中的数据点来查看详细信息。	项	1
38			比对结果可视化	为更直观地呈现数据比对的结果，提供数据可视化展示的功能。通过图表、地图、热力图、时间轴等形式，将复杂的比对结果以易于理解的方式展示出来。案件的发生地点可以通过地图标注进行展示，案件时间的分布可以通过时间轴展示，数据间的相关性可以通过散点图或者网状图进行显示。	项	1
39			动态更新与及时反馈	具备动态更新比对结果并实时反馈的能力。当新证据或新数据加入时，可以自动重新计算并更新比对结果。	项	1
40		数据下载与导出	数据下载	提供下载功能，允许将比对结果导出为常见的数据格式，如 Excel、PDF 等。方便警务人员保存分析数据，也能为后续的工作提供数据支持。	项	1
41			数据导出	根据不同的需求，支持自定义导出格式。可以选择导出特定的数据列、筛选条件或者可视化图表的图片等。	项	1

42	刑事科学技术提示	案件类型识别与分类	识别与分类	通过自然语言处理(NLP)技术分析报案描述或案件记录，自动将案件分类为盗窃、诈骗、凶杀等不同类型，实现自动分类管理。	项	1
43			处理建议	提供特定的技术应用指南或合理化建议，如针对网络犯罪可能推荐数字取证工具，而对实体犯罪则侧重于 DNA 分析或指纹比对。	项	1
44		提供相关辅助技术支持	勘察建议	利用图像识别技术分析犯罪现场的照片或视频，帮助识别潜在的证据点如脚印、血迹位置等，并给出相应的采集建议，辅助现场勘查。	项	1
45			案件还原	根据案件发生的地点和时间条件（如天气、光线），进行环境模拟或重建现场，协助调查人员更好地理解事件发生的过程。	项	1
46		刑事技术手段提示	法医鉴定建议	对于涉及身体伤害的案件，提供详细的法医鉴定步骤和技术要求，辅助法医鉴定指导，确保准确评估伤情及死亡原因。	项	1
47			物证收集建议	根据具体案情提出合理的物证收集、保存和检验方案及物证处理建议，如何正确提取并保存电子设备中的数据作为证据。可结合心理学理论和实际案例，通过分析嫌疑人作案手法、选择目标的特点等信息，绘制心理画像，为侦查工作指明方向。	项	1
48	实战案例模型构建	人物关系网络构建	人物关系提取	利用自然语言处理(NLP)技术分析文本资料（如口供记录、社交媒体信息等），自动识别并提取出涉及的人物及其相互之间的关系（如亲属、同事、朋友等）。	项	1
49			图形化展示	将识别出的关系以图形化的形式呈现出来，形成一个人物关系网络图。每个节点代表一个实体（个人或组织），边表示两者间的关系强度或类型。以便于警务人员快速理解案件中的关键人物及其联系。	项	1
50		数据关联与挖掘	数据关联	从多个来源收集数据，包括但不限于电话记录、财务交易、监控视频等，实现多层次数据整合并将其整合到统一平台上进行分析。	项	1
51			数据挖掘	进行深度学习算法应用，使用机器学习和深度学习算法来发现隐藏在大量数据背后的模式和规律，如异常的资金流动路径可能暗示非法活动的存在。	项	1
52		关键节点与优先级标注	关键节点标注	根据预先设定的标准（如涉案程度、社会影响力等），对人物关系网络中的关键节点进行高亮显示，实现重要节点突出，使决策者能够迅速聚焦于最重要的嫌疑人或证人。	项	1
53			优先级标注	系统可以基于新获得的信息动态调整各节点的重要性评分，实现动态调整权重，确保关注焦点始终集中在最具价值的目标上。	项	1
54		助力破案实战推演	侦查初期分析	通过信息技术手段助力破案，提升案件侦破的速度和准确性。在初期侦查阶段，可快速梳理所有相关方的基本信息及相互间的关系，绘制出初步的人物关系图谱。	项	1
55			侦查中期分析	深入挖掘每一笔可疑交易背后的资金流向，结合通话记录等其他证据材料确定核心团伙成员；在后期锁定目标阶段，可依据不断更新的线索重新评估各嫌疑人的威胁等级，集中力量抓捕首要分子。	项	1
56			侦查后期分析	可依据不断更新的线索重新评估各嫌疑人的威胁等级，集中力量抓捕首要分子。	项	1
57	辅助知识智能检索	智能化案件资料管理	资料归档	利用自然语言处理技术对案件文档进行分析，自动为新加入的证据材料建立索引并分类归档。	项	1
58			资料关联	通过语义理解和文本分析，识别不同案件文档之间的潜在联系，进行关联性分析，帮助执法人员快速找到相关的证据或信息。	项	1
59		个性化调证方	调证模型构建	基于车辆、嫌疑人等多维度信息建立动态积分模型。	项	1

60		向建议	生成建议	为执法人员提供针对性的调证建议。如对于高风险目标可能推荐更深入的背景调查或者特定类型的证据收集。	项	1
61		辅助追踪追溯资金流向	资金流向模型构建	支持辅助对资金流向追踪，如通过冠字号进行智能检索和分析，将极大提升办案效率，特别是在调证过程中针对特定交易或事件的调查。如通过整合银行系统中的冠字号数据，系统可以快速定位涉案资金的流动路径，辅助警方锁定嫌疑人。	项	1
62	决策分析支持	犯罪预测与预警	犯罪预测与预警模型构建	利用机器学习算法，构建犯罪预测与预警模型。	项	1
63			生成建议	根据过往犯罪记录和社会经济因素预测未来可能发生犯罪的时间和地点，以优化警力配置。通过分析大量的历史案件数据、社会媒体信息和其他公开资源，发现潜在的犯罪模式和趋势，帮助警方提前部署预防措施。	项	1
64		风险分析评估	风险评估	对于特定个体或群体，通过分析其行为特征来评估潜在的安全威胁。	项	1
65			监控策略	制定相应的监控策略。	项	1
66		重大活动方案制定	活动信息处理	支持处理大量复杂的信息，为指挥中心提供决策支持。	项	1
67			应对方案生成	在大型活动安保或突发事件处理过程中，系统可以综合考虑多方面因素，给出最佳应对方案。	项	1
68		智能调度与资源配置	警力智能调度	基于当前的治安状况和预测模型，系统可以动态调整警力部署，确保在最需要的地方有充足的资源可用，优化警力分配。同时在突发事件中，系统可以协助指挥中心快速评估形势并制定最佳响应计划，包括调动适当的资源和人员。	项	1
69			警力资源调配	在突发事件中，系统可以协助指挥中心快速评估形势并制定最佳响应计划，调动适当的资源和人员。	项	1
70		社区警务与互动	安全状况报告	通过收集和分析社区内的各类数据，系统可以生成关于该地区安全状况的报告，进行社区安全评估，帮助社区成员了解所在环境的风险点。	项	1
71			互动服务平台	面向公众的服务平台，比如失踪人口搜索、失物招领等功能，加强警民之间的沟通和信任。	项	1
72	数字证书安全管理	智能保管系统	警员管理	警员列表可以对证书警员进行添加、导入、导出、修改等功能。同时可查看警员人脸识别认证的照片信息，单位列表可添加、修改、删除警员所属单位的相关信息。	项	1
73			证书管理	证书管理包含：证书列表、使用详情、绑定关系、修改证书申请列表、修改证书审批列表。	项	1
74			证书柜管理	设备列表可对证书柜进行查看、添加、删除、修改等。同时可查看证书柜内的证书信息。 使用日志可以查看证书柜的使用日志信息。	项	1
75			审批管理	审批管理可对相关的申请进行审批，查看申请内容。	项	1
76			台账管理	台账管理包含：辅警借用及申请表、民警借用及申请表、辅警绑定及申请表。	项	1
77		数字证书安全管理	警员管理	通过同步按钮手动从警员 LDAP 上按照系统管理员配置的更新策略同步更新警员用户列表，解析警员数字证书，从中获取证书 SN，从 DN 中解析出警员姓名、身份证号和机构代码并从机构表中获取对应的机构名称，注册时间为该警员记录添加时间。可对警员账号进行新增、删除、冻结和解冻，操作之后需要更新推送该警员的安全任务策略。	项	1
78			辅警管理	通过同步按钮手动从辅警 LDAP 上按照系统管理员配置的更新策略同步更新辅警用户列表，解析辅警数字证书，从中获取证书 SN，从 DN 中解析出辅警姓名、身份证号和机构代码并从机构表中获取对应的机构名称，注册时间为该辅警记录添加时	项	1

				间。可对辅警账号进行新增、删除、冻结和解冻，操作之后需要更新推送该辅警的安全任务策略。		
79			任务管理	显示警员对辅警下发的所有安全任务信息，查看安全任务明细并且可以编辑、结束任务，结束时如果是执行中的安全任务需要选择任务结束方式是完成还是中止。	项	1
80			账号源管理	账号同步策略和警员账号源的管理，设置同步账号的更新方式、间隔时间的同步策略，并对警员和辅警账号的 LDAP 地址、端口配置（默认值：389）、BaseDN、用户 DN 和用户口令等进行安全配置，支持 LDAP 连通性测试，并显示测试结果。	项	1
81			认证管理	对服务进行认证管理，通过对应的服务地址及端口上传对应的许可证文件。	项	1
82			业务审计	以表格形式显示警员的操作日志记录。业务日志用于审计所有警用数字证书安全管理系统服务接口的流水日志，并且可用于分析是否有可疑访问或恶意的攻击。	项	1
83			管理审计	以表格形式显示管理员的操作日志记录。操作日志可用于审计所有警用数字证书安全管理系统的管理操作日志。	项	1
84			机构管理	对警员及辅警的所属机构进行管理，可通过标准模板进行导入和手动新增。	项	1

2.硬件部分

序号	设备名称	配置	数量	单位
1	通用服务器	处理器：配置 2 颗高性能多核处理器，单颗处理器物理核心数≥20 核，处理器基础主频≥2.0GHz，三级缓存≥27.5MB。 内存：标准配置总容量≥256GB DDR4 或更高规格 ECC 内存；最大可扩展内存容量不低于 512GB。 硬盘：配置≥2 块 480GB SATA SSD 系统盘；配置≥3 块 8TB SATA HDD 数据盘；最大支持 8 个 3.5 英寸/2.5 英寸热插拔硬盘位。 网卡：板载≥4 个千兆电口；配置≥2 个万兆 SFP+光口，并随设备提供相应数量的万兆多模光模块。 RAID 卡：配置硬件 RAID 卡，缓存≥1GB 或性能相当的无缓存硬件方案，支持 RAID 0、1、5、6、10、50、60。 接口：提供≥2 个 USB 3.0 接口；≥1 个 VGA 接口；≥1 个 RJ45 独立管理网口。 扩展：提供≥6 个 PCIe 3.0 或以上标准扩展插槽。 电源：配置 1+1 或以上冗余电源，支持电源智能管理、功耗封顶等功能。 机箱：标准 2U 机架式服务器。 软件与兼容性：设备需预装或兼容主流企业版 Linux 操作系统（需提供长期技术支持版本）及 Windows Server 操作系统，并提供全套驱动程序。 节能与认证：产品需符合中国节能产品认证标志，投标时须提供国家确定的认证机构出具的、处于有效期内且覆盖所投产品型号的节能产品认证证书。	10	台
2	GPU 服务器	处理器：配置 2 颗高性能多核处理器，单颗处理器物理核心数≥24 核，处理器基础主频≥2.0GHz，三级缓存≥100MB 内存：标准配置总容量≥512GB DDR4/DDR5 ECC 寄存式内存；最大可扩展内存容量≥1.5TB，以确保为 GPU 运算提供充足数据缓冲。 硬盘：系统盘：配置≥2 块企业级 NVMe SSD，单盘容量≥960GB，组建 RAID 1 以保障系统可靠性。 数据盘：配置≥4 块大容量企业级数据盘，其中至少 2 块须为高性能 NVMe SSD（单盘容量≥3.84TB），其余为 SATA/SAS HDD（单盘容量≥16TB），裸容量总和≥80TB。 网卡：板载≥4 个千兆电口；额外配置：≥2 个万兆 SFP+光口及≥2 个 25G SFP28 光口（需随箱提供相应数量的万兆及 25G 多模光模块）。 RAID 卡：配置缓存≥4GB 并集成掉电保护功能的高性能硬件 RAID 卡，支持 RAID 0、1、5、6、10、50、60。 接口：≥2 个 USB 3.0 接口；≥1 个 VGA 接口；≥1 个 RJ45 独立管理网口。	1	台

		GPU 扩展：支持安装并全带宽（x16 Lane PCIe 4.0）运行≥8 块全高全长双宽 GPU 加速卡 单卡性能要求：FP32 计算性能 ≥ 40 TFLOPS；INT8/Tensor 性能 ≥ 320 TOPS（用于 AI 推理）；显存容量 ≥ 24GB 电源：配置额定功率≥2700W 的 2+2 冗余钛金标准电源，以满足满配 GPU 峰值功耗。 散热：配置高效散热系统，支持 N+1 冗余热插拔风扇，确保在满配 GPU 且持续满载运行时，于工作温度 10° C-35° C、相对湿度 8%-90%（非冷凝）环境下稳定工作。 管理功能：提供完整的 IPMI2.0 远程系统监控、远程 KVM、虚拟媒体等各种管理功能。 软件与兼容性：设备需预装或兼容主流企业版 Linux 操作系统（需提供长期技术支持版本）及 Windows Server 操作系统，并提供全套驱动程序。		
3	数字安全管理证书柜	支持生物特征识别（如人脸、指纹），实现 U-Key 与用户身份绑定，实现数字证书的存放与取用。取用、归还证书时，均会对柜体操作人员进行拍照，可在管理平台查看。能判别插入柜体 USB 接口的是否为真实有效公安数字证书，并能读取证书号（ID），且不允许对证书进行加工或者外置设备来鉴别证书。提供存取日志及行为分析功能。柜门数量为 20 个。证书的容纳要求包括不限于以下类型：非国密的塑料外壳证书、非国密金属 A1 版证书、非国密金属 B1 版证书、国密金属 A1 版证书。需符合国家生物信息安全管理规范。具备公安部安全与警用电子产品质量检测中心颁发的检验报告。	10	台
技术规格说明： 1.本文件所列技术参数为最低要求，允许投标人提供性能等同于或优于所列规格的产品进行应答。 2.投标人须在应答文件中针对所有“≥”条款，明确其所投产品的具体规格，并提供产品官方技术白皮书或官网截图作为证明。 3.本项目所投所有硬件设备，均须提供自验收合格之日起不少于 3 年的原厂质保及 7×24 小时技术服务支持。此项承诺须在投标文件中以原厂服务承诺函的形式加盖原厂公章。				

3.合同包 1 特有要求

3.1 人员配置要求

为确保项目质量与进度，供应商须组建具备 AI 技术背景的专业团队。

（1）项目负责人(1 名)：5 年以上 AI 或大型知识管理系统项目管理经验；

（2）AI 算法专家(1 名)：精通 NLP、知识图谱、机器学习等领域；

（3）自然语言处理工程师(2 名)：负责法律语义理解、实体识别等核心 NLP 模块开发；

（4）知识图谱工程师(1 名)：负责法律知识图谱构建与可视化；

（5）全栈开发工程师(3 名)：负责前后端开发，精通主流前端框架与后端微服务架构；

（6）数据工程师(1 名)：负责非结构化数据的清洗、结构化处理与向量化；

（7）测试工程师(1 名)：具备 AI 模型评测经验。

3.2 设施设备配置要求

（1）开发与测试环境：

供应商需自建具备高性能 GPU 计算能力的开发测试环境，单卡显存不应低于合同包 1 中 GPU 服务器配置的 70%，用于 AI 模型的训练与调优。

需搭建与生产环境网络策略一致的仿真环境，用于系统集成测试。

（2）数据处理与存储：开发测试环境需配备足以容纳全部法律条文、历史案例及模拟数据的数据存储与处理能力。

（3）采购人提供条件：采购人提供符合等保要求的机房环境、公安网接入及必要的办公条件。

3.3 运维服务要求

（1）质保期：提供自最终验收合格之日起不少于 3 年的免费质保期。

（2）AI 模型运维：

模型更新：提供至少每季度一次的 AI 模型优化与迭代服务，根据使用反馈提升智能体的准确性与智能化水平。

知识库更新：提供法律法规、典型案例知识库的月度增量更新服务，确保系统知识的时效性。

系统监控：提供 7×24 小时系统运行状态监控，保障智能体服务的持续可用性。

3.4 技术支撑服务

（1）响应机制：

严重故障（系统无法访问、核心功能失效）：30 分钟内响应，2 小时内提出解决方案并启动应急处理。

一般故障（部分功能异常，不影响主流程）：2 小时内响应，8 小时内解决。

（2）技术支持内容：提供远程技术支持和必要的现场技术支持，确保系统稳定运行。提供针对 AI 模块的专项技术支撑，包括模型效果评估、参数调优咨询等。

3.5 培训要求

（1）管理员培训：培训内容包括系统架构、用户与权限管理、AI 模型管理、知识库维护、系统监控与日志审计等。不少于 16 课时。

（2）最终用户培训：面向一线警务人员，培训重点为 AI 警务智能体的各项功能实操，如智能检索、流程指引、案例参考等。采用案例教学，不少于 24 课时。

（3）培训材料：提供全套中文培训手册、操作视频及模拟演练环境。

（二）合同包 2（打击网络赌博及网赌涉案关系网络分析系统建设）

1.软件部分

序号	模块	功能项	二级功能	功能描述	单位	数量
1	涉案	构建涉案人	单人分析模型	建立网赌、网络诈骗涉案人员单人分析模型。	项	1

	人员单人关系分析	员单人分析模型	构建			
2			社交圈分析	显示分析网赌、网络诈骗涉案人员的直接社交圈。	项	1
3			重要度分析	简单直观的体现网赌、网络诈骗涉案人员个人社交圈结构，并发现网络中不同人的重要程度。	项	1
4			关系圈区分	智能区分分析对象的不同关系圈。	项	1
5		涉案人员单人关系网络展现	社交挖掘和聚类	对给定人员的核心身份标识（如身份证号、手机号等）在指定的分析时段内的一级关系所形成的社交网络进行挖掘和聚类，发现出组织中不同的人所处的重要程度。	项	1
6			来源地分析	对组织中所有人员进行来源地判断，进行标签化展示。	项	1
7			社交网络呈现	以可视化的方式将社交网络进行呈现。如分析某涉案人员，可以发现其关系网络构成部分、核心联系人及其涉案人员等。	项	1
8	涉案人员群组分析	构建涉案人员群组分析模型	群组分析模型	建立网赌、网络诈骗涉案人员群组分析模型。	项	1
9			群组关系分析	对给定的一批没有规则核心身份标识(如身份证号、手机号等）人员进行社交关系分析，能够挖掘发现隐藏在这些关系网络中的组织结构，并能发现各群组内成员详细情况和群组中的重要节点。	项	1
10			人员构成分析	通过对一些重要节点进行分析往往能发现问题的重要线索。再结合核心身份标识（如身份证号、手机号等）的标签信息即可以判断每个群组的人员构成和群组属性。	项	1
11		涉案人员群组关系网络展现	关系网络挖掘	给定一组人员的核心身份标识（如身份证号、手机号等），对这些核心身份标识（如身份证号、手机号等）在指定的分析时段中存在的组织进行挖掘，对能形成组织的各组织内其他成员进行发现。	项	1
12			重要节点发现	发现组织中的重要节点，并且可以选择是否隐藏不重要节点，从而实现涉案人员群组分析。	项	1
13			可视化呈现	可视化形式呈现。如掌握一批涉案核心身份标识(如身份证号、手机号等），可以对其进行分析，可以得到其组织结构、敏感核心人、核心联络组织、敏感中间人、结合两组指标可以发现其隐藏背后的幕后中高层成员等。	项	1
14	涉案人员关系呈现	涉案人员关系呈现	社交网络聚类	给定一组人员的核心身份标识（如身份证号、手机号等），对这些身份证号在指定的分析时段内的一级关系所形成的社交网络进行聚类。	项	1
15			详单抽取	对给定一组号码根据给定的时间段范围在对应的关系特征库表中进行详单抽取，对抽取的数据进行简单的过滤。	项	1
16			抽取数据过滤	对抽取的数据进行简单的过滤，然后根据过滤后的数据直接进行关联信息和所相关的所有核心身份标识（如身份证号、手机号等）的计算。	项	1
17			可视化呈现	显示它们相互间的关系和他们各自的直接联系人，以可视化的方式将社交网络进行呈现。	项	1
18	涉案人员关联发现	涉案人员关联发现	最短联系路径挖掘	给定一组人员的核心身份标识（如身份证号、手机号等），深入挖掘两个身份证号、手机号或多个身份证号、手机号间的最短联系路径，发现之间的隐匿关联关系。	项	1
19			最短路径发现	推荐他们之间最多的最短路径，并发现整体的关系网络结构。如输入某涉案人员核心身份标识（如身份证号、手机号等），则可分析出其在城市通过哪些中间人及中间组织，补全其灰色产业链的构成部	项	1

				分等。		
20			可视化呈现	显示它们相互间的路径关系，以可视化的方式将关系网络进行呈现。	项	1
21	涉案人员社团扩展	建立社团扩展分析模型	模型设计	建立社团扩展分析模型，当用户仅仅只掌握了一个网赌、网络诈骗涉案团体中的几个人或者部分人时，可以通过此模型分析发现这些对象所在团体中的其他成员。此模型用于网赌、网络诈骗涉案同伙发现。	项	1
22			可视化呈现	显示它们相互间的路径关系，以可视化的方式将关系网络进行呈现。	项	1
23		涉案人员社团关系网络展现	模型设计	建立社团关系网络展现模型，给定一组人员的核心身份标识（如身份证号、手机号等），对这些核心身份标识（如身份证号、手机号等）在指定的分析时段内共同所在的同一组织中的其他成员的发现。	项	1
24			可视化呈现	以可视化的方式将社交网络进行呈现。如掌握一批网赌、网络诈骗人员，则可以深层挖掘出其潜在的其他涉案人员。	项	1
25	建立涉案人员/团伙画像	涉案嫌疑人数据画像	标签化嫌疑人信息	将嫌疑人信息分类并予以标签化，通过聚合分析、抽象出嫌疑人信息全貌，服务于侦查工作。	项	1
26			数据处理	通过公安内网、社会行业数据、大数据公司、个人电子设备等数据源，获取涉案嫌疑人基本数据，然后运用数据挖掘技术分析、归纳和提炼这些数据的特征。	项	1
27			画像展示	标签化展示其立体形象，刻画出嫌疑人和相关人的身份、行为特征、兴趣爱好、人际关系全貌。	项	1
28		涉案犯罪团伙数据画像	数据处理	从某个案件或者涉案嫌疑人出发，通过讯问、摸排找到整个团伙，由面到点式地挖掘出核心团伙、核心成员。对全量数据进行采集、清洗和要素提炼。	项	1
29			侦查情报知识图谱构建	对需要关注的人、对象及其显、隐性关系，编织为侦查情报知识图谱。	项	1
30			团伙数据画像	监视目标人物的行动轨迹、日常活动，运用社群查找法，根据其与其他成员的联系强度，找出关联群体。将群体的行为模式导入预测型类罪模型，自动识别其可疑度并匹配相适应的预警标识。运用社会网络分析法，分析高度可疑群体的组织架构和通信流，运用活跃度、中介度、中心度等算法，挖出犯罪团伙的关系链条、幕后操纵者和核心成员。发现每个成员的角色、作用、成员间的关系及分工合作情况，通过用户关联分析法理清子团伙组织结构。	项	1
31	人员标签管理	构建人员标签库	建立标签库	建立人员标签库，标签库可分为基本属性、公共管理、涉赌涉诈几大类。	项	1
32			标签库编辑	可根据案件需要建立不同小类标签。	项	1
33			标签库更新	所有的标签按天更新、按周更新、按月更新、按年更新。	项	1
34		标签基础管理	标签创建	提供标签的创建服务。	项	1
35			标签配置	标签与或非操作、配置专题标签、标签更新等功能。	项	1
36			标签操作	标签的创建、编辑、删除及分类。	项	1
37			自定义标签	允许用户自定义标签名称、层级关系和属性值。根据对网赌、网络诈骗涉案嫌疑人或犯罪团伙的数据分析，用于后续对对应的核心身份标识（如身份证号、手机号等）的所有标签信息的支撑。	项	1
38		标签检索与查询	/	根据标签碰撞结果，提供各类标签的检索与查询。支持通过标签名称、内容关键词及多标签叠加筛选和检索。	项	1

39	空间分析	位置分析	/	对于存在位置信息的对象，如行程信息、归属地、住址，可在地图上进行位置分析，显示位置信息，直观发现空间上的联系。	项	1
40		轨迹分析	/	对于存在位置轨迹的信息的对象，如行程，寄递，GPS 轨迹，可在地图上动态显示轨迹（结合时序分析，时间和空间结合更直观发现线索）。	项	1
41	图标库	实体图片	/	根据不同实体类型对象，显示不同类型的图片，如：人，车，电话，银行卡等。	项	1
42		属性图片	/	根据属性区别，显示不同的图片，如：男，女，恐怖分子，目标人物，毒贩，头目等。	项	1
43	危险目标提醒	/	/	将标注的危险目标进行监控，危险目标有新的信息（如：通话信息，行程信息，汇款信息），以消息的形式推送提醒，掌握危险目标最新的动态。	项	1
44	数据接入	实施自动对接	/	对于通联类的实时数据，通过实时流计算技术，实时将原始数据进行清洗计算和入库，实现数据实时自动对接。	项	1
45		批量图形化导入	/	对于通过文件方式存储的原始数据，可以在系统 UI 界面上进行批量图形化导入，支持 txt、excel、csv 等文件格式。	项	1
46	系统管理	用户管理	用户基本信息设置	用来统一管理系统所需的用户信息，包括用户列表、用户基本信息设置、用户账号管理等。	项	1
47			用户管理	用户管理提供用户维护、注销、停用、单点登录等功能。	项	1
48		角色管理	角色管理	角色管理提供系统用户角色维护、角色分配、角色撤回等功能，用于将系统用户和权限实现控制。	项	1
49		权限管理	权限资源管理与控制	权限管理将系统中所有用户和权限资源进行统一集中的管理和权限控制，实现对用户的鉴权及功能权限控制。	项	1
50	系统日志审计	系统日志审计	日志审计	记录系统的日志并进行日志审计。日志审计范围包括全部用户和重要的安全相关事件，包括用户标识与鉴别、访问控制的所有操作记录。	项	1
51			资源使用记录	记录系统资源的异常使用、重要系统命令的使用等。	项	1

2.硬件部分

序号	设备名称	配置	数量	单位
1	通用服务器管理平台	1.服务器资产管理：可支持手动、自动扫描和批量导入新增服务器。支持服务器信息(处理器、内存、硬盘、网卡、RAID 卡、风扇、电源等)采集和配置。可以对操作系统无关的远程对服务器的完全控制，包括远程的开关机、重启、更新固件、配置；支持对服务器信息导出。支持固件批量升级。 2.服务器资产统计：可以支持服务器设备和部件的分类统计及明细查询。 3.首页大屏：支持首页大屏展示，可以在一个页面展示设备数量，设备告警统计，设备健康统计，可以监控设备 CPU 温度、设备功率、cpu 内存使用率；可视化显示 TOP5 情况，一个页面可监控相关信息并支持跳转相关页面。实现风险的可视化管控。 4.告警管理：支持查看当前告警，历史告警，事件信息，以及配置告警规则，告警通知对象。支持通过告警级别、告警内容、告警状态等内容筛选展示告警数据，实现便捷化运维管理。支持通过邮件和短信形式及时通知运维人员。支持 SNMP 上报电源等硬件异常状态。 5.服务器设备定位：支持通过序列号搜索定位服务器或相关部件的位置，方便故障设备或部件定位。 6.主机性能监控：支持服务器运行数据监控，包括 CPU 使用率、CPU 负载、TOP10 进程 CPU 使用率、内存使用率、TOP10 进程内存使用率、磁盘空间使用率、磁	1	套

		盘读写带宽、磁盘 IOPS、网络带宽、网络包速率、GPU 温度、GPU 功率、GPU 使用率、GPU 风扇速率、GPU 显存使用率等相关监控数据。 7.传感器监控：支持服务器可视化传感器(温度传感器、风扇传感器和电源传感器)监控。传感器数据包括但不限于传感器名称、传感器状态、传感器值、过低严重告警阀值、过低轻微告警阀值、过低故障阀值、过高严重告警阀值、过高轻微告警阀值、过高故障阀值、采集时间等相关监控数据。 8.GPU 监控：支持 GPU 的全面监控，支持 GPU 温度、GPU 功率、GPU 利用率、GPU 风扇使用率、GPU 显存使用率、XID 错误号、PCIe 传输速率、SM 时钟频率、修正的 ECC 错误总数、热限制违规的时间等共计 100 余项。 9.知识库：内置默认的平台运维知识信息，可以提问题、写文章、和根据关键字全文检索。可对集群常见问题进行归纳管理。支持 word、pdf 等附件上传。 10.值班管理：支持运维人员排管管理，值班信息记录。通过可视化图表形式直接对人员和班次进行设置与管理。值班人员可以直接查看到个人排班计划并可在系统中直接记录相关情况。管理人员可批量查看值班记录。		
2	通用服务器	处理器：配置 2 颗高性能多核处理器，单颗处理器物理核心数≥20 核，处理器基础主频≥2.0GHz，三级缓存≥27.5MB。 内存：标准配置总容量≥256GB DDR4 或更高规格 ECC 内存；最大可扩展内存容量不低于 512GB。 硬盘：配置≥2 块 480GB SATA SSD 系统盘；配置≥3 块 8TB SATA HDD 数据盘；最大支持 8 个 3.5 英寸/2.5 英寸热插拔硬盘位。 网卡：板载≥4 个千兆电口；配置≥2 个万兆 SFP+光口，并随设备提供相应数量的万兆多模光模块。 RAID 卡：配置硬件 RAID 卡，缓存≥1GB 或性能相当的无缓存硬件方案，支持 RAID 0、1、5、6、10、50、60。 接口：提供≥2 个 USB 3.0 接口；≥1 个 VGA 接口；≥1 个 RJ45 独立管理网口。 扩展：提供≥6 个 PCIe 3.0 或以上标准扩展插槽。 电源：配置 1+1 或以上冗余电源，支持电源智能管理、功耗封顶等功能。 机箱：标准 2U 机架式服务器。 软件与兼容性：设备需预装或兼容主流企业版 Linux 操作系统（需提供长期技术支持版本）及 Windows Server 操作系统，并提供全套驱动程序。	10	台
3	国产防火墙	1.性能参数：网络层吞吐量≥4G，应用层吞吐量≥2G，并发连接数≥200 万。 2.硬件参数：国产化芯片及国产化操作系统，产品不少于 6 个千兆电口，内存不小于 8G，硬盘不小于 128G SSD，1U 机箱。 3.支持虚拟防火墙的创建、启动、关闭、删除功能；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、安全策略等功能。 4.支持链路探测，能够在每接口上以 PING/DNS/ARP/BFD 等协议探测目标主机可达性，探测链路是否有效。 5.支持静态路由、策略路由和多播路由协议以及 BGP、RIP、OSPF 等动态路由协议。 6.支持多对一、一对多和一对一等 NAT 方式以及 NAT44 、NAT64、NAT66 地址转换方式。 7.支持多维度访问控制，维度包含：网络区域、网络对象、MAC 地址、服务、应用、域名等。 8.支持管理安全策略，可以管理以及审计安全策略修改的时间、原因、变更类型。 9.产品支持 X-Forworded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁。（需提供证明材料并加盖厂商公章）。 10.支持 OWASP 定义 10 大 web 安全威胁防护，保护服务器免受基于 Web 应用的攻击,SQL 注入防护、XSS 攻击防护、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护，内置 WEB 应用攻击特征。（需提供产品功能截图并加盖厂商公章） 11.提供 3 年产品升级、规则库升级、软件升级服务。	1	台

4	国产化上网行为管理	1.性能参数：网络层吞吐量≥2Gb，应用层吞吐量≥150M，带宽性能≥100M，支持用户数≥500；每秒新建连接数≥1000，最大并发连接数≥50000。 2.硬件参数：国产化芯片及国产化操作系统，规格：1U，内存大小≥8G，硬盘容量≥128G SSD，接口≥6 千兆电口。 3.能够识别和分类各种 URL 类型，同时所有 URL 类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制；（需提供功能截图并加盖厂商公章） 4.支持对 Web 请求访问情况进行检测，可对内网用户使用 web 请求访问网络流畅情况进行检测，通过质量评级对整体网络进行展示； 5.支持包括 WEB、FTP、SMB 类型业务内容以及行为做审计，对上传/下载文件可选择只审计文件名或同时审计文件内容； 6.支持超过千种以上的主流 Saas 应用，且对 Saas 应用有默认的分类标签，帮助客户统一配置策略；（需提供功能截图并加盖厂商公章） 7.能够识别和分类各种 URL 类型，同时所有 URL 类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制；（需提供功能截图并加盖厂商公章） 8.支持对具体用户、账号和终端等信息设置流量配额，维度精确到日和月，当配额耗尽后，将对应用户加入到指定的流控黑名单惩罚通道中；（需提供功能截图并加盖厂商公章） 9.支持在邮件收发上设置安全策略，可允许用户登录 Webmail 收邮件，但不能发送 Webmail 邮件；（需提供功能截图并加盖厂商公章） 10.提供 3 年产品升级、规则库升级、软件升级服务。	1	台
5	国产化安全资源池硬件平台	1.硬件要求：国产化芯片及国产化操作系统，不少于 2 颗 CPU；CPU 核数≥32；内存≥128G；系统盘≥2*240GB SATA SSD，缓存盘≥2*480G SSD，数据盘≥16T ；千兆电口≥4 个；万兆光口≥2 个； 2.平台包含数据库审计组件、运维审计组件、日志审计组件、漏洞扫描等安全功能组件； 3.可通过现有模板直接部署组件，比如出口边界安全、等保合规等； 4.可以通过拖拽设备图标及画图的方式，完成网络拓扑的搭建，实现快速搭建整个业务逻辑的能力，并且可以实现网络设备的开启、关闭和连接；（需提供产品界面截图，并加盖厂商公章） 5.平台首页可以一体化展示设备主机状态、磁盘状态及应用状态，以及业务和用户遭受的安全风险、待处理的系统事件等相关安全信息； 6.可根据实际业务需求，划分安全区域，简化运维管理；（需提供产品界面截图，并加盖厂商公章） 8.提供 3 年产品升级。	1	台
6	国产化安全资源池软件	国产化数据库审计软件 1.数据库流量≥100M。 2.深度解码数据库网络传输协议，完整记录用户数据库会话细节，包括发生时间、源 IP、源端口、源 MAC、目的 IP、目的端口、数据库用户、数据库类型、操作类型、SQL 语句、SQL 模版、客户端程序名、响应码、影响行数、返回行数、SQL 预计响应时间； 3.内置大量 SQL 安全规则；支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断；. 4.支持 SNMP 方式，提供系统运行状态给第三方网管系统；支持 Syslog 方式向外发送审计日志； 国产化日志审计软件 1.性能参数：包含资产授权数量≥50 个。 2.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等多种日志源不少于 800 种日志对象的日志数据采集。支持对日志源的批量采集和日志源数据的批量转发。 3.支持对单个/多个日志源批量转发，支持定时转发，可通过 syslog 和 kafka 方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。	1	套

		4.支持拓扑管理，能够基于拓扑图的资产相关数据信息快速查看资产评分、安全事件分布、告警分布等，支持通过拓扑下钻查看对应资产的关联事件、审计事件、日志数量。 5.支持个性化定制，支持全系统更换 logo 与系统名称，支持一键恢复默认。支持 POC 测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险。 国产化堡垒机软件 1.提供≥20 个资源授权。 2.提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能。 3.支持通过批量导入、导出、编辑等进行资源管理，支持手动查询资源、添加资源、编辑资源、删除资源等操作。 4.支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人。 5.支持临时运维操作流程启动、关闭，当出现紧急事件时可以设置紧急访问路径直接运维设备，同时系统会自动留痕记录工单信息 6.支持对于 linux、Unix、网络设备高危命令执行审批操作，可以指定对应运维人员命令审批人，保证运维操作安全性。同时支持对于 select、drop 等 SQL 语句执行进行语句阻断； 7.支持对于图形资源审计回放，可以从键盘、剪切板、窗口标题、文件传输记录等不同维度设置访问回放； 国产化漏洞扫描软件 1.授权：系统漏扫授权 IP 数≥50。 2.支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。 3.支持从紧急漏洞的视角展示主机风险，清晰呈现已发生和未发生的紧急漏洞类型，支持以报表形式展示紧急漏洞的风险等级、影响资产数、漏洞数量、最近发现时间，可关联漏洞详情。 4.支持漏洞扫描、WEB 扫描、弱口令、安全基线检查、变更检查的五合一任务，五者也可任意组合执行任务。 5.支持对周期任务的多次任务执行结果进行比对，比对结果中详细展示报告间的异同之处。 6.支持三权分立方式的授权，即管理员只负责完成设备的系统配置，安全管理员负责配置核查，审计员负责对系统本身的用户操作日志管理和审计。		
7	国产化杀毒	1.软件版授权≥80。 2.支持针对局域网内所有的终端资产进行统一的排查和清点，并且进行快速风险评估，评估内容包括不仅限于：操作系统、应用软件、监听端口和终端账户。 3.具备攻击故事完整链条的展示能力，可自行通过进程树溯源展示出攻击开始到当前节点的所有行为，协助网络安全人员进行安全事件攻击溯源和研判分析； 4.支持网络环境下主机安全风险可视化，包括但不限于：高级威胁、僵尸网络、WebShell 后门、高危漏洞等模块; 5.要求在发生勒索事件时，主机客户端可执行自动删除原始文件夹中被勒索病毒加密的文件夹，同时主机客户端可对敏感文件或文件夹进行隔离；（需提供产品功能截图证明并加盖厂家公章） 6.要求主机安全服务端平台具备主机的系统层、应用层行为业务流量数据精细化采集能力，相关数据采集面至少应覆盖 ATT&CK 技术面 163 项；（需提供产品功能截图证明并加盖厂家公章） 7.主机安全软件支持从资产维度实时展示资产的风险状态，并给出加固会整改建议；（需提供产品功能截图证明并加盖厂家公章） 8.为保证安全防护效果杀毒软件可以与本次提供防火墙之间进行联动处置，	1	套

		防火墙可联动杀毒软件进行一键查杀。（需提供产品功能截图证明并加盖厂家公章）。 9.提供3年软件升级服务。		
技术规格说明： 1.本文件所列技术参数为最低要求，允许投标人提供性能等同于或优于所列规格的产品进行应答。 2.投标人须在应答文件中针对所有“≥”条款，明确其所投产品的具体规格，并提供产品官方技术白皮书或官网截图作为证明。 3.本项目所投所有硬件设备，均须提供自验收合格之日起不少于3年的原厂质保及7×24小时技术服务支持。此项承诺须在投标文件中以原厂服务承诺函的形式加盖原厂公章。 4.国产化证明：合同包2清单中序号3至7的“国产化”设备及软件，投标产品须符合国家关于信息技术应用创新产品的相关标准与规范，并提供由国家认可的权威检测认证机构出具的、能够证明其所投具体产品型号的国产化兼容性、安全性与可靠性的测试报告或认证证书。				

3.合同包2特有要求

3.1 人员配置要求

本项目团队需突出大数据分析与图计算能力。

（1）项目负责人(1名)：5年以上大数据分析或关系网络类项目管理经验；

（2）系统架构师(1名)：精通分布式系统架构、图数据库技术；

（3）大数据开发工程师(2名)：负责数据接入、清洗、ETL流程开发；

（4）图计算算法工程师(2名)：负责关系网络分析、社团发现等核心图算法研发；

（5）前端开发工程师(2名)：专注于多维数据可视化交互实现；

（6）后端开发工程师(2名)：负责系统微服务、API接口开发；

（7）安全工程师(1名)：负责系统安全加固、渗透测试。

3.2 设施设备配置要求

（1）开发与测试环境：

供应商需自建具备大规模数据处理和图计算能力的开发测试环境，其数据存储与计算节点规模不应低于生产环境的50%。

需搭建包含图数据库（如Neo4j, Nebula Graph）、大数据平台（如Hadoop/Spark）的完整测试环境。

（2）数据仿真：必须建立高度仿真的测试数据工厂，模拟生成符合网赌、网络诈骗特征的通讯、交易、社交关系等数据，严禁使用真实涉案数据。

（3）采购人提供条件：采购人提供符合等保要求的机房环境、公安网接入、及与相关业务数据库进行联调测试的协调支持。

3.3 运维服务要求

（1）质保期：提供自最终验收合格之日起不少于3年的免费质保期。

（2）数据与规则运维：

数据接口维护：保障与各类数据源接口的稳定连通，负责接口变更的适配工作。

分析模型优化：提供至少每半年一次的分析模型与规则库优化服务，根据新型犯罪手法调整特征识别策略。

（3）系统监控：提供 7×24 小时系统及数据流监控，重点关注数据入库延迟、图查询性能等核心指标。

3.4 技术支撑服务

（1）响应机制：

严重故障（数据入库中断、分析引擎崩溃）：30 分钟内响应，2 小时内提出解决方案。

一般故障（可视化展示异常、查询速度慢）：2 小时内响应，1 个工作日内解决。

（2）技术支持内容：提供远程和现场技术支持。提供针对复杂关系网络分析需求的专项技术咨询，协助办案人员深度挖掘数据关联。

3.5 培训要求

（1）系统管理员培训：培训内容包括系统架构、数据源管理、用户权限管理、图数据库维护、系统监控与审计等。不少于 20 课时。

（2）数据分析师培训：面向情报研判人员，深度培训关系网络分析、社团发现、画像构建等高级功能的实战应用技巧。采用真实案例复盘教学，不少于 32 课时。

（3）操作员培训：面向一线办案民警，培训系统基本查询、人员档案查看、线索上报等操作。不少于 16 课时。

（4）培训材料：提供全套中文培训手册、典型战法案例集、系统操作视频。

四、项目通用要求

（一）实施期限与性能要求

1.项目实施期限：合同签订生效且具备实施条件之日起 60 日历天内完成全部系统的开发、部署、上线调试，并达到初步验收条件。

2.系统性能要求：核心业务系统页面平均响应时间不超过 3 秒，关键事务处理成功率不低于 99.9%。

（二）付款方式

1.合同签订后，达到付款条件起 30 日内，支付合同总金额的 30.00%；

2.项目全部系统开发部署完成，通过初步验收并上线稳定运行，达到付款条件起

30 日内，支付合同总金额的 50%。

3.项目最终验收合格后，达到付款条件起 30 日内，支付合同总金额的 20%。

（三）验收标准

1.项目验收应依据本采购需求文件、中标人的投标文件及承诺、双方签订的合同以及国家、行业相关标准进行。

2.验收内容包括但不限于：

(a)所有软硬件产品的数量、品牌、型号、配置应与合同约定一致。如供应商因产品更新换代等原因需提供替代产品，应事先书面征得采购人同意，且替代产品的性能指标、技术规格及兼容性不得低于原合同约定；

(b)软件系统所有功能模块均实现并达到采购需求文件规定的功能描述和技术指标；

(c)系统运行稳定，性能指标达到采购需求文件规定的服务标准；

(d)中标人已按合同约定提交完整的技术文档和培训资料；

(e)提供符合要求的培训服务。

3.验收分为初步验收和最终验收。初步验收在系统部署调试完成后进行，最终验收在系统试运行期满 3 个月进行。

（四）通用服务与政策要求

1.文档交付：项目验收前，中标人需向采购人交付完整的项目实施文档、系统操作手册、维护手册、接口规范等技术资料。

2.强制采购政策：

合同包 1、合同包 2：本合同包硬件要求中的通用服务器为强制节能产品，供应商须提供国家确定的认证机构出具的、处于有效期内的节能产品认证证书，且认证证书需包含本次所投产品的具体型号，否则按无效投标处理。

3.节能环保产品政策：供应商所投产品属于“节能产品政府采购品目清单”或“环境标志产品政府采购品目清单”内的，应提供由国家确定的认证机构出具的、处于有效期内的、覆盖所投产品具体型号的节能产品认证证书或环境标志产品认证证书。

4.数据安全与保密责任：中标供应商在项目开发、测试、部署及运维的全过程中，必须建立并执行严格的数据安全管理规范，对接触到的任何采购人业务数据、仿真数据及系统信息负有严格的保密责任，不得用于与本项目无关的任何目的。项目结束后，须按采购人要求彻底清除所有相关数据。

5.公平竞争与技术开放性说明

本采购需求文件中所有技术参数、功能描述及人员能力要求，均旨在明确项目目标与质量所需。允许投标人基于其技术路线，提供性能等同、功能等效或更优的解决方案进行应答。文件中出现的任何品牌名称、特定产品或技术栈，均应理解为对一类产品或技术的示例性描述，而非强制要求。

五、采购人提供条件

采购人负责提供项目实施所需的基本现场条件，包括：

1.符合国家标准的机房环境（承重、供电、空调、消防、防静电）。

2.稳定、不同断的电力供应（UPS）。

3.符合要求的机柜空间、网络布线及连接至公安信息网的网络接入。

4.项目实施期间固定的办公场所及必要的办公设施。

5.必要的物理门禁与安保措施。

白水县公安局

2025 年 10 月 15 日