达州市政务一体化移动警务跨网交互通道建设项目初步报价函

达州市公安局：

根据贵单位《达州市政务一体化移动警务跨网交互通道建设项目初步询价函》相关项目需求，结合我司产品特点和相关项目实施经验，初步报价如下表所示：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 产品 | 参数要求 | 是否符合需要 | 单价（万元） | 数量 | 报价（万元） |
| 万兆交换机 | 1、三层以太网交换机主机（标准机架式设备），带WEB网络管理功能，标配不少于8个千兆GE电口+14个1/10G SFP光口插槽 Plus端口，实配≥4个万兆多模光模块；2、交换容量不低于2.56Tbps/23.04Tbps，包转发率220Mpps，实配≥1个USB接口3、实配1个交流电源模块 |  |  | 2 |  |
| 万兆防火墙 | 1、标准机架式机构，配置千兆电口≥2个，千兆光口≥2个，万兆光口≥2个及对应模块，≥1个可扩展槽，网络吞吐率≥20Gbps，最大并发连接数≥500万，支持扩展IPS入侵防御、WAF、URL过滤及AV防病毒功能，配置双冗余电源；2、符合网络安全等级测评三级要求；（投标人需提供承诺函并加盖投标人公章）3、内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供产品功能界面截图，并加盖投标人公章） |  |  | 1 |  |
| 服务器 | 1. 2U机架式服务器；国内知名品牌，自主研发，国内拥有相应的研发机构。2. CPU：配置≥2颗英特尔至强第三代可扩展处理器，CPU核心数≥16核，主频≥2.4GHz。3. 内存：配置≥64GB 3200MHz DDR4内存，最大支持16根DDR4内存，最高速率3200MT/s；4. 阵列控制器：配置外插高性能8通道SAS Raid卡；支持raid 1/0/10/5/50/6/60； 5. 本地存储：系统盘配置≥1块240G SSD 企业级固态硬盘；数据盘配置≥2块4T 7.2K SATA 3.5寸企业级热插拔硬盘；6. PCIE插槽：支最大支持5个标准PCIE插槽加1个OCP3.0卡;最大支持4个单宽GPU卡；7. 网络：配置≥2个千兆网口，支持OCP3.0网络模块，支持1/10/25/40/100/200 GE网卡；8. 电源及外设：配置≥2个550W电源；冗余散热风扇，机架安装导轨；9. 为保证元数据节点的数据安全性，元数据节点设备厂商需通过服务器类的IEC61340-5-1静电防护标准认证，提供设备厂商在全国认证认可信息公共服务平台的官网截图予以证明，并加盖投标人鲜章；10. 为保证底层信息系统计算安全，可满足等保3.0标准对计算环境安全防护要求；投标设备支持同品牌主机安全增强系统防护，符合《信息安全技术 操作系统安全技术要求 GB/T 20272-2006》，提供CNAS或CMA认可，第三方权威机构出具的主机安全增强系统检测报告复印件，并加盖投标人鲜章；11.为保证数据存储安全，存储节点硬盘采用具备知识产权的防震硬盘托架，解决存储节点在使用过程中由于震动引起的磁头盘片碰撞，造成的数据丢失的问题； |  |  | 5 |  |
| 执法仪 | 2.8寸彩屏、4G/3G网络、北斗/GPS定位、POC语音对讲、WiFi、蓝牙、NFC、可旋转镜头拍摄、无线肩咪、3500mAh锂电池、IP68 |  |  | 30 |  |
| 智能眼镜 | 适用于巡逻盘查，重大安保活动等场景，提供便捷的可视可查功能。通过usb连接警务通，实现佩戴式人脸捕捉。 |  |  | 15 |  |
| 人脸核验一体机 | 通过采集人脸相关信息，经移动警务通道进入人像库比对，在公安网可实现实时预警。 主要功能：人脸捕获上传、多图人脸同时抓拍、全景监控、云台、交互显示、支持有线、4G联网。 |  |  | 1 |  |
| 移动式人证核验一体机 | 双屏人像抓拍核验设备可实时抓拍人脸图像或读取二代身份证信息并抓拍人脸图像，通过人脸对比技术，实现对通行人员的实人实证信息的快速核验。主要功能：标准模式核验、极速模式核验、重点人员比对预警、本地布控比对预警、核验记录统计查询95% |  |  | 1 |  |
| 融合计算系统（服务端） | 包含音视频通信服务、通信融合服务、融合定位服务、数据计算服务、北向接口服务1. 音视频通信服务2. 通信融合服务（1）应用层：通过调用通信融合平台标准统一接口，可为上层应用平台提供音频、视频、位置、短信、数据类的业务通信功能、调度功能。（2）接口层：接口层主要为上层应用包括指挥调度平台、接处警平台、勤务平台等提供对接接口，接口形式包括API/Webservice/ActiveX等形式。（3）平台层：提供语音、视频、短消息、位置信息的调度服务，包括信令解析、信令交换与控制、媒体转换、媒体融合等服务。3. 融合定位服务（1）支持以卫星定位能力为基础，融合基站、WIFI特征值、蓝牙等定位技术进行综合定位，提高定位精度，并能实现室内室外全域定位。（2）通过精准定位、持续定位，将终端位置基础信息进行全面处理，生成元素包，服务于警员位置上图、指挥巡防位置采集、重大活动安保岗位签到等应用模块的定位上图。4. 数据计算服务（1）边缘计算：包含图片解析算法和视频解析算法，与本地重点人员库或常口库数据对接，获取人员识别能力，并应用于移动警务终端、4G/5G执法记录仪等无感盘查场景中应用；（2）视觉计算：将视图解析数据统一汇聚到大数据平台，对视图解析数据进行结构化处理，生成人脸、人体、车辆等专项数据，结合大数据平台资源池，生成视图档案、实名轨迹、通信类数据轨迹等轨迹信息，并对外提供视觉计算能力。（3）大数据平台接入：实现于大数据平台的对接，大数据平台对警情分级，因案授权、因事授权，按警情等级不同，展示不同的查询内容，并将结果返回至总线。总线将查询结果按级返回至警务终端。5. 北向接口服务（1）基础模块：负责第三方系统的登入、登出、获取通信融合一级平台内的组织架构数据、终端个号数据、组号数据及各种上下线的消息推送。（2）管理模块：负责会议、群组、动态重组功能的新增、修改、删除操作。 |  |  | 1 |  |
| 融合计算系统（PC端） | 视频画面调取：通过点击地图标注点，即可调取在线的前端设备（移动警务终端、智能眼镜、执法记录仪等）拉取实时视频画面，并以大图的方式呈现，供指挥人员决策调度。音视频呼叫：通过点击地图上的设备（移动警务终端、执法记录仪、PDT终端)实现点对点即时语音呼叫和视频呼叫。并根据群组范围及权限，用户可以进行语音组呼功能和切换群组功能。音视频通信1、语音呼叫 用户可以通过拨号或通讯录选取联系人的方式，对通联对象进行语音呼叫，语音呼叫支持点对点或点对多呼叫。2、视频呼叫 用户可以通过拨号或通讯录选取联系人的方式，对通联对象进行视频呼叫，语音呼叫支持点对点或点对多呼叫。3、点呼根据权限，用户可以选择权限范围内的人员信息，实一对一的视频和语音呼叫。4、组呼根据群组范围及权限，用户可以进行语音组呼功能和切换群组功能。 |  |  | 1 |  |
| 融合计算应用APP | 融合通讯：建设后端与前端的一张图可视化指挥调度能力，基于前端的终端建设、后端的平台服务，指挥中心可随时了解现场情况，通过单呼、组呼、群呼、视频拉取、视频分发、位置信息等功能与一线完成信息通信的交互，一线民警可通过警务通、执法仪、PDT等服务能力完成与指挥中心的信息交互。佩戴眼镜，实现快速比对、无感盘查。 |  |  | 1 |  |
| 万兆移动应用管理系统 | 一、物理配置：必须配合万兆移动应用代理系统使用：1、标准机架式设备；网口：不低于2个千兆网口、不低于2个万兆网口；电源：500W单电源；二、功能要求：1、多种应用支持：持B/S应用，支持FTP、telnet、远程桌面以及通用的C/S应用，支持UDP应用(通过服务器接入服务)；；2、多服务功能：系统具备多种服务，保护不同的类型接入服务；3、DNS代理功能：外部客户端可以直接使用内部域名访问应用，系统通过HTTP头将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息；（需提供系统功能截图，并加盖投标人公章）4、策略统一下发：系统实现客户端策略的统一下发，用户无需对客户端进行任何配置；5、错误重定向：系统对于认证错误可以重定向到用户指定页面，增强友好性；6、基于证书的角色转换：在移动接入中可以将外部证书角色自动转换为公安内部证书角色，保证业务的连续性；7、对原有https应用灵活支持：可以采用穿透模式和证书转换模式实现对原有https应用的灵活支持；（需提供系统功能截图，并加盖投标人公章）8、系统备份恢复功能：系统可以备份当前所有配置，保证系统瘫痪时的快速恢复；9、恢复出厂设置功能：系统具有恢复默认设置功能，方便使用；10、系统在线升级：系统支持Web方式的系统升级；11、性能检测功能：系统支持对CPU、内存、磁盘容量、连接数、进程等资源情况的收集，便于系统的维护和问题定位；12、高可靠性：支持双机热备功能；三、性能要求：1、支持并发连接数：不低于5000个；2、新建连接数：不低于5000个；3、最大吞吐量（国密算法）：不低于5Gbps； |  |  | 1 |  |
| 万兆移动应用代理系统 | 一、物理配置：必须配合万兆移动应用管理系统使用：1、标准机架式设备；网口：不低于2个千兆网口、不低于2个万兆网口；电源：500W单电源；二、功能要求：1、多种应用支持：持B/S应用，支持FTP、telnet、远程桌面以及通用的C/S应用，支持UDP应用(通过服务器接入服务)；；2、多服务功能：系统具备多种服务，保护不同的类型接入服务；3、DNS代理功能：外部客户端可以直接使用内部域名访问应用，系统通过HTTP头将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息；（需提供系统功能截图，并加盖投标人公章）4、策略统一下发：系统实现客户端策略的统一下发，用户无需对客户端进行任何配置；5、错误重定向：系统对于认证错误可以重定向到用户指定页面，增强友好性；6、基于证书的角色转换：在移动接入中可以将外部证书角色自动转换为公安内部证书角色，保证业务的连续性；7、对原有https应用灵活支持：可以采用穿透模式和证书转换模式实现对原有https应用的灵活支持；（需提供系统功能截图，并加盖投标人公章）8、系统备份恢复功能：系统可以备份当前所有配置，保证系统瘫痪时的快速恢复；9、恢复出厂设置功能：系统具有恢复默认设置功能，方便使用；10、系统在线升级：系统支持Web方式的系统升级；11、性能检测功能：系统支持对CPU、内存、磁盘容量、连接数、进程等资源情况的收集，便于系统的维护和问题定位；12、高可靠性：支持双机热备功能；三、性能要求：1、支持并发连接数：不低于5000个；2、新建连接数：不低于5000个；3、最大吞吐量（国密算法）：不低于5Gbps； |  |  | 1 |  |
| 万兆网闸 | 1、标准机架式设备,内外端机双侧液晶屏；内端机≥6个千兆电口，≥4个千兆光口，≥2个万兆光口，≥1个扩展槽位； 外端机内端机≥6个千兆电口，≥4个千兆光口，≥2个万兆光口，≥1个扩展槽位；,冗余电源,网络吞吐量≥7Gbps； 并发连接数≥40万；内外端机≥1TB硬盘。2、系统内部采用“2+1”模块结构设计，即包括内端机、外端机和专有隔离硬件，管理接口位于内端机上，通过该接口进行产品配置，外端机上无管理口；3、支持并具备安全浏览、文件传输、文件同步、邮件访问、VOIP访问、数据库访问、数据库同步、自定义访问等功能；4、支持基于IP地址、端口、时间以及源用户身份的访问控制策略，支持最大活动会话数的控制和统计，支持IPV6扩展头的安全设置； 5、支持黑白名单访问控制基于单一域名，支持基于URL分类地址库的访问控制，支持允许、阻断、告警三种处理方式；（提供截图证明，并加盖投标人公章）6、支持HTTP安全功能，支持URL过滤引擎、内容过滤引擎、文件过滤引擎、病毒过滤引擎、网页过滤引擎安全防护及单独启用或停用控制；7、支持增量式计算校验和的方法，保障数据在摆渡传输过程中的连续性；（提供截图证明，并加盖投标人公章）8、具备文件同步功能，支持基于文件大小和文件修改时间的同步策略，支持手动指定上下限阈值；（提供截图证明，并加盖投标人公章）9、提供基于FTP协议和TFTP协议的文件传输功能，可过滤FTP协议内的命令、数据层内容，处理方式包括允许、阻断、告警等； |  |  | 1 |  |
| 万兆防火墙 | 1、标准机架式机构，配置千兆电口≥2个，千兆光口≥2个，万兆光口≥2个，≥1个可扩展槽，网络吞吐率≥20Gbps，最大并发连接数≥500万，支持扩展IPS入侵防御、WAF、URL过滤及AV防病毒功能，配置双冗余电源；2、支持一体化安全策略配置，可以通过一条策略实现五元组信息源MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT等功能配置,简化用户管理；3、支持手工链路聚合及LACP链路聚合，提供不少于10种的负载分担算法，灵活实现对聚合组内业务流量的负载分担，提高链路可靠性；（需提供系统功能截图，并加盖投标人公章）4、符合网络安全等级测评三级要求；（投标人需提供承诺函并加盖投标人公章）5、支持基于特征进行流量识别，利用机器自学习能力实现加密流量识别，发现加密流量中的泄密信息；（需提供中华人民共和国国家知识产权局出具的专利证书，并加盖投标人公章）6、访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址；7、内置异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供产品功能界面截图，并加盖投标人公章）8、支持对设备CPU、内存、磁盘、整机流量、新建、并发进行统计，展示设备CPU、内存、硬盘实时利用率及其历史走势图； |  |  | 3 |  |
| 网络准入认证系统 | 一、物理配置：标准机架式设备1、接口配置：不低于6\*GE+4\*SPF+2\*10G SFP+；2、CPU：不低于8核 2.2GHz；内存：DDR4 不低于16G频率；硬盘：不低于500G SATA；二、功能要求：1、部署模式：支持与多形态终端安全管理系统联动对接实现网络准入管控，支持与省厅移动警务算法认证系统及加密机联动对接实现终端白名单认证准入控制；（需提供相关对接承诺，并加盖投标人公章）2、网管方式与网管策略：支持以HTTP及SSL加密的Web图形化接口进行设备配置和管理，支持英语、简体中文、繁体中文接口；SSH管理：支持 SSH 命令行管理方式；支持Console管理。3、网络功能：支持静态路由功能；支持本地DNS配置；支持源地址转换，端口映射，一对一映射；支持应用层网关，FTP，SIP（GB28181），RTSP，H.323等。4、终端状态：支持列出在线已准入终端列表，并支持查询；支持列出已准入并离线的终端，并支持查询；支持列出私接终端，并支持查询；支持列出仿冒终端，并支持查询；支持列出风险终端，并支持查询；支持列出已阻断终端，并支持查询。5、终端管理：对已经准入的终端进行管理，并支持分组；支持根据国产密码算法认证结果、IP网段，终端类型，对终端进行自动准入，并分配到不同的分组；对私接终端，仿冒终端可以选择阻断或者是仅记录日志；支持根据VLAN，IP网段对流量进行放通。（提供产品功能界面截图，并加盖投标人公章）6、风险评估：支持主动扫描发现终端的安全漏洞，并有针对视频终端的漏洞库；支持FTP，TELNET，SSH，RTP等协议的弱口令扫描。7、应用协议识别：支持识别GB28181，ONVIF，RTP，厂商私有视频等视频协议；识别HTTP，FTP、SMTP、TFTP、IMAP等常用协议；HTTP多线程下载、伪IE下载等多种方式的HTTP下载等进行识别；FTP上传文件、FTP下载文件、FTP命令；QQ远程协助、SSH、Windows远程桌面、VNC、TeamViewer等。数据库 DB2、MySQL、Oracle、SQL等；支持视频资源访问日志，记录访问的视频资源地址，访问来源。8、统计功能：支持对视频网络流量监测，不用基于7层应用识别的应用流量排行，包括视频等流量；支持对视频网络流量监测，可显示摄像头流量排行；对全网总体流量进行统计，以趋势图展示；支持对每个物理接口的流量进行统计，以趋势图展示；支持对系统本身CPU，内存的等的使用率进行统计；支持对终端个数进行统计，统计上线的终端个数。9、告警、日志报表：对于事件日志，DOS，IPS，病毒查杀等日志配置告警；记录每条连接的会话日志，同时也记录DOS日志，IPS漏洞防护日志，病毒查杀日志等；统计攻击来源，安全统计，设备资源，区域统计，网络流量服务类型统计等；管理统计日志数据的存储策略，查看数据列表，数据备份等功能。（提供产品功能界面截图，并加盖投标人公章）10、集中管理：支持外置集中管理平台，可以通过外置集中管理平台管理设备，下发策略，升级版本，监控设备运行状态等；支持发送日志和统计到集中管理平台进行统一存储和展示。三、性能要求：1、应用层吞吐量2G，最大接入端数≥5000；并发≥1000； |  |  | 1 |  |
| 移动警务多形态终端证书 | 1、算法安全：提供数据加解密、数字签名、数字信封等密码运算服务，支持AES、DES、3DES、SM2、SM3、SM4等国密及国际相关密码运算。2、密钥安全：基于可密钥重构技术，实现了密钥与算法的融合，可以为每个不同的用户生成不同的算法实例。3、协议安全：支持双向认证和会话密钥协商。4、环境检测：终端应用程序在每次运行时需要对自身完整性和SDK完整性进行联机动态较验。5、可信程序检测：终端应用程序在每次运行前，会进行联机动态进行完整性校验。6、运行环境检测：终端应用软件通过安全插件检测到运行环境处于ROOT 或者已越狱等非安全环境时，向用户进行环境安全警示，必要时可终止运行。7、抗攻击能力：安全插件具备抵御静态分析、动态调试、进程注入等基本的抗攻击能力。8、安全沙箱：终端的安全插件运行在沙箱内了有独立的进程保护，在终端形成独立的软件数据防护区域，关键数据防重放，防篡改。9、安全加固：安全插件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。 |  |  | 32 |  |
| 多形态终端安全管理地市节点 | 1、资产管理1.1、资产分类管理：可将终端分为不同类型的资产，不同类型终端支持不同的管理策略。1.2、终端类型管理：根据终端具体形态、厂家、型号、功能等信息支持创建不同的类型模板。（需提供系统功能截图，并加盖投标人公章）1.3、终端注册管理：终端在使用前进行登录注册，需在平台添加相应的终端注册信息，终端注册信息包括终端名称、所属组织、终端类型、是否公用、终端标识码、ICCID、APN模板等。1.4、终端管控管理：在终端注册成功以后，在平台中可看到全部终端的状态，包括终端ID、终端名称、终端类型、所属组织、终端状态、终端标识码、IMEI/MEID、设备型号、ROM版本号、配发状态、在线、失联、ROOT、最后连接时间等。（需提供系统功能截图，并加盖投标人公章）1.5、终端分组管理：平台支持创建不同的终端分组，通过分组进行策略管理。1.6、终端上报功能：终端支持硬件资产、软件资产、限制状态的上报。2、策略管理2.1、终端配发：终端在使用前，需要进行终端配发，指定使用人员或者组织。2.2、模板管理：支持限制模板和消息模板两种，限制模板根据不同终端类型打开相关限制项，消息模板可自定义具体消息内容。（支持禁用相机、禁用麦克风、禁用定位、强制启用定位、禁用蓝牙、启用蓝牙白名单、禁用WLAN、启用WiFi白名单、禁用飞行模式、禁用个人热点、禁用OTG存储、禁用大容量存储、禁用SD卡\NM卡、禁用安装、禁用截屏、禁用录屏禁用USB调试、禁止修改系统时间、启用锁机、启用水印、启用机卡绑定、启用登录认证）2.3、策略管理：支持消息模板、地理围栏、强制安装、应用黑名单、静默卸载、应用防停止、客户端防卸载等不同策略管控终端。（需提供系统功能截图，并加盖投标人公章）2.4、执行跟踪：支持查看策略的执行状态明细。2.5、初始化设置：支持给新注册终端初始化策略（包括第一次注册和重新注册的终端）。初始化设置可根据组织机构进行配置。3、组织人员管理3.1、组织管理：支持批量导入、手工添加两种方式添加组织机构。3.2、人员管理：支持批量导入、手工添加两种方式添加人员。3.3、用户登录：支持多形态终端登录，支持登录认证配置。4、黑白名单管理4.1、WiFi白名单:开启WiFi白名单功能后，仅允许连接白名单内的WiFi；关闭白名单时，允许连接所有WiFi。4.2、蓝牙白名单：开启蓝牙白名单功能后，仅允许连接白名单内的蓝牙设备；关闭蓝牙白名单时，允许连接所有蓝牙设备。4.3、USB白名单：开启USB白名单时，仅允许连接白名单内的USB设备；关闭白名单时，允许连接所有USB设备。5、应用管理5.1、分类管理：对上传应用，可进行应用分类管理。5.2、应用管理：支持应用上传、应用审批、应用分配、应用下架、应用删除等全生命周期管理。5.3、应用防卸载：支持应用防卸载功能。6、配置管理6.1、二维码配置：支持通过服务器地址、推送地址、卡片编号和APN配置等信息，生成二维码。（需提供系统功能截图，并加盖投标人公章）6.2、二维码模板：支持生成每个人员的注册二维码。6.3、客户端管理：支持进行客户端上传、发布、更新管理。7、报表统计7.1、支持终端报表、应用报表、管理员日志、限制状态报表、应用使用情况报表、终端使用报表。8、系统设置8.1、角色管理：支持管理员角色化区分，可根据管理员职能分配相应的功能权限。8.2、管理员管理：支持对管理员进行增、删、改、查、角色分配等操作，支持多级管理员，上级管理员可管理下级管理员信息，下级管理员不可管理与查看上级或平级管理员信息。8.3、系统参数设置：支持设置登录页Logo、网络配置、系统参数配置、客户端参数设置。9、终端安全管理9.1、恢复出厂：支持恢复出厂功能。9.2、禁用硬重置：支持终端禁用硬重置。9.3、禁用软恢复：支持终端禁用软恢复；禁用OTA：支持禁用OTA；手动取消激活：支持手动取消激活。10、支持多形态终端安全管理授权≥200011、与省厅内网多形态终端安全服务端对接，实现多形态终端策略管控，管控功能不限于WIFI、蓝牙、USB等；（需提供相关对接承诺，并加盖投标人公章） |  |  | 1 |  |
| 融合计算一体化应用组件 | 通过安装或集成的方式植入警务通终端、执法记录仪等多形态终端设备，通过对接融合计算后台服务系统，获取音频、视频、位置、组织数据、群组数据等数据资源，并赋予终端设备相关音视频通信、指挥调度、人脸识别等功能。支持与终端安全管理系统服务端实时联动，下载移动警务终端控制策略并执行，主动预防各类违规事件发生。结合移动警务网络建设特点，全方位保障移动警务终端使用环境安全性。支持通过采集设备软硬件设备指纹提取特征，根据设备指纹特征生成的与设备匹配绑定的唯一密码模块，有效了防止了账户欺骗与设备仿冒。 |  |  | 47 |  |
| 移动警务集中管控子系统 | 1、监测审计1.1、通过对二类区的防火墙、核心交换机、应用服务器等通用及专用设备的基础性能状态的指标采集，实现平台内所有设备健康观测和性能监控分析等功能；（提供产品功能界面截图，并加盖投标人公章）1.2、通过对移动终端的设备状态信息、应用安装信息、应用运行信息、终端违规事件、指令执行记录的采集；能够对审计数据进行提取、清洗、关联、比对、标记等处理；通过构建自动分析模型，当安全事件发生时，系统能自动发现攻击、违规和异常行为并告警；通过分类展示及数据查询等统计分析界面，在发生安全事件后，管理人员可快速关联到访问对象、访问行为、访问过程和事件产生原因；1.3、通过对应用系统的用户身份鉴别行为、用户访问应用行为、应用访问资源行为、用户应用授权信息、应用资源授权信息和应用状态等信息的采集；提供分类展示及数据查询统计分析界面，当发生异常行为和安全事件时可告警提醒，并提供行为事件的详情回溯；1.4、对移动警务平台内所有的使用机构及人员状态信息及与机构人员关联的其他管控要素进行安全审计；对移动警务平台个服务区内服务资源状态信息、资源授权信息、应用访问资源信息等进行安全审计并提供分类展示和多维查询功能；2、资产管理通过agent、snmp和api接口的方式采集移动警务平台内各类资产信息，实现移动警务平台用户、终端、基础设施、应用系统、资源服务等全要素资产信息的注册、变更和统计，构建资产分类、资产属性、资产关系三位一体的动态资产模型，实现资产模型数据的可定义、可编辑、可扩展，并支持通过网络拓扑进行资产关系管理；（提供产品功能界面截图，并加盖投标人公章）3、态势感知对用户、终端、网络、应用、服务资源等管控要素进行安全信收集整理，整合系统安全事件、系统漏洞等信息，基于因果关系和安全事件关联等技术进行安全态势评估，实现对安全风险、安全威胁的溯源处理，动态调整运行参数和安全策略模型，实现精准有效的安全管理；4、集控数据中心实时高效地接入移动警务平台内个管控对象的动态时序指标及日志数据，包括设备基础监控指标、终端登录日志、应用性能要求各类IT运维数据，对这些运维数据进行低成本存储、高效计算、关联分析建模，并通过接口的方式，为上层应用和三方系统提供各类数据支持服务；（提供产品功能界面截图，并加盖投标人公章）5、统一告警对来自于平台内各管控要素包含设备状态的告警消息、应用性能告警消息、日志传输告警消息及其他自定义告警进行统一的接入与处理，支持告警事件的过滤、通知、响应、处置、定级、跟踪以及多维分析，实现问题事件全生命周期的全局管控；6、可视化大屏在公安网集中管控平台建设本地集中管控可视化大屏；  |  |  | 1 |  |
| 移动警务集中管控系统采集器 | 1、采集通用网络设备的运行状态，包括CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等；2、采集服务器的运行状态，包括CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等；3、采集通用安全设备的运行状态，包括CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等；4、采集专用安全设备的运行状态，包括CPU、内存、网络等使用情况以及由系统产生的各类异常告警信息等，专用安全设备的业务日志信息；5、采集系统本身的业务运行日志、管理员管理操作日志以及系统告警信息等；6、支持对采集的数据按照后台系统提供的规则进行数据清洗、整理、抽取、归一、统计、分析等基本数据处理；7、所有数据支持上报移动警务集中管控系统；8、本次采集并发授权数≥50； |  |  | 1 |  |
|  | 合计 |  |

本事项联系人：黄警官 联系电话：2115210

公司名称（盖章）

二〇二二年 月 日