第五章　采购需求

一、采购标的

1. 采购标的

为北京市外地罪犯遣送处提供移动警务服务。

2.项目概述

为满足北京市外地罪犯遣送处的狱内狱外移动执法、指挥调度、即时沟通、快速查询、远程办公等需要，促进工作效率、执法水平和监管执法能力的进一步提升，不断推动执法工作移动化、智能化目标的实现，打造一体化移动警务模式。包括移动执法终端服务、移动执法 5G 专网服务、光纤传输链路及网络传输设备服务、移动警务管控平台服务、语音流量通讯服务、移动执法网络安全服务。

二、商务要求

1. 交付（实施）的时间（期限）和地点（范围）

自服务时间开始之日 12 个月。具体服务数量及服务期限如下。

序号	单位名称	数量（人）	服务期限（月）	预算金额（万元）
1	北京市外地罪犯遣送处	536	12 个月	128.64

投标人所提供服务的最高限价为 200 元每人每月。服务期内如有人员增加，中标人接到通知后，须提供相同的移动警务服务。

实施地点：北京市外地罪犯遣送处

2. 付款条件（进度和方式）

北京市外地罪犯遣送处与中标人签署合同并根据每月实际使用人数据结算。以支票或汇款形式结算，具体结算方式以最终签订合同支付条款为准。

3. 包装和运输

如适用，须满足《关于印发〈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）〉的通知》（财办库〔2020〕123 号）

三、技术要求

投标人提供的移动警务服务内容应满足北京市监狱管理局关于移动警务使用管理的相关要求和《司法行政系统移动执法系统技术规范》（SF/T0049-2020)的相关技术要求。

1、移动执法终端服务

1.1 移动执法终端

终端应选用国产品牌，如果所投服务的终端产品停产或无法供货的情况下，要升级到同系列的下一代产品。依据司法部移动执法终端技术标准和实际的使用需求，终端选型标准参数如下：

芯片

CPU：核数不低于 8 核，主频不低于 3.2GHz；

内存：不低于 16GB RAM+512G ROM；

显示屏

尺寸：不低于 6.73 英寸，多点触控触摸屏；

色彩：不低于 10.7 亿色，支持 DCI-P3 广色域；

分辨率：不低于 FHD+ 2800 x 1264 像素；

屏幕像素密度 PPI：不低于 453PPI；

尼特值不低于 3000 nit；

刷新率：支持 120hz；

摄像头

后置摄像头：最高主摄不低于 5000 万像素，支持可变光圈、光学变焦、OIS 光学防抖，支持闪光灯及自动对焦；

前置摄像头：不低于 3200 万像素广角摄像头；

其他功能

蓝牙：不低于 BT5.3，支持 BLE、SBC、AAC、LDAC、APTX、APTX HD

感应器：加速度传感器、接近光传感器、指纹传感器、支持（屏内指纹），支持指纹解锁、指南针、陀螺仪、重力传感器、后置色温传感器，单点激光；

网络通讯：双卡，双待，双通，支持全网；

支持移动/联通/电信 5G/4G+/4G/3G/2G；

语音：具有通话功能；

NFC：内置 NFC 模块，支持读卡器模式，卡模拟模式；

电池：容量不低于 5000Ah，支持快充，充电功率不小于 66W；

电池续航能力：可支持执法终端连续工作不低于 8 小时，待机时间不低于 72 小时；

防护要求：六面可承受 30 厘米高度跌落水泥地面及 80 厘米跌落至木地；

支持 PWM 调光、护眼模式、自然色彩显示；

1.2 执法终端配件

执法终端全部配置手机保护壳和钢化屏幕保护贴膜；

1.3 终端售后维护服务

依据执法终端生产厂商的售后服务标准执行；

2、移动执法 5G 专网服务

2.1 监管区内移动执法专网

建设覆盖北京市外地罪犯遣送处监管区内的移动执法专网，满足移动执法终端在监管区内进行执法活动的业务需求。具体如下：

实现专用网络建设：通过在监管区部署专用基站的方式，为监管区构建快速、可靠的 5G 执法专网，满足高安全性、高可靠等定制化建网需求。

实现监管区全覆盖：监所监管区内（监所围墙内）室内和室外移动 5G 执法专网覆盖，监管区内移动执法专网覆盖的区域达到 95%以上；

实现业务隔离：为监管区内业务提供专用业务数据通道，实现流量的定向汇聚，确保数据安全，移动执法专网与公网信号采用不同 DNN 接入点，执法网流量通过专用光纤链路与市局网络实现安全连接，保障监管区内执法应用的安全访问；

移动执法专网专用接入服务：监管区内 5G 执法专网只有指定的移动执法终端且在监管区模式下才能接入，其它终端或其它模式无法接入；

保障监管区内移动执法终端在管控下能够正常使用语音通信服务；

配置的专用 UPF 等设备应采用双机热备的方式部署，提供支持设备运行不低于 2 小时的不间断电源；

移动执法专网应根据业务发展预留资源，综合考虑系统升级和下一代通信系统的演进；

2.2 监管区外移动执法专网服务

移动执法终端位于监管区外时，通过专用 DNN 连接公用基站方式实现民警通过移动执法终端在全国范围内对业务系统安全访问的需求。

实现业务隔离：执法终端在监管区外通过接入专用 DNN，业务数据通过公用基站接入，

将用户业务流通过专线与市局网络实现安全连接，保障监管区外办公应用的安全访问；

实现安全接入：执法终端在监管区外接入执法专网时应通过数据分流的方式，实现与公网业务的安全隔离，并经由安全认证后允许接入；

保障移动执法终端在监管区外正常使用语音通信、收发短信等通讯服务

2.3 移动执法终端互联网访问服务

移动执法终端在监管区外切换为个人模式后，业务数据通过运营商公用基站，实现互联网访问服务。

3、光纤传输链路及网络传输设备服务

依据北京市监狱管理局（北京市戒毒管理局）智慧城市规划（2023-2025 年）以及移动执法和业务系统的实际需求，移动执法链路传输专线服务需要满足如下需求：

提供北京市外地罪犯遣送处到市局机关裸光纤链路 1 条，传输带宽 10Gb，并配置相应的传输设备，满足业务需求并具备扩容能力；

基于裸光纤传输的链路要求可以根据业务需求，北京市外地罪犯遣送处可以在传输链路上开通不少于 4 个业务端口，并配置对应的网络传输模块，用户可以自行根据业务需求配置不同业务端口的带宽。

配置传输网管系统，实现业务电路调度，电路开通及调配。实时监控链路的工作状态，完成电路质量分析，保障链路的安全可靠，由采购人管控。

提供北京市外地罪犯遣送处执法网网络核心交换设备，满足万兆带宽的数据传输需求，并为后期业务增加提供扩容空间;

提供支撑传输和网络设备所需的不低于 2 小时运行的不间断电源。

4、移动警务管控平台服务

4.1 移动执法终端管控系统

移动执法终端管控系统由安全监控组件和后台移动执法终端管理服务器组成。

安全监控组件运行于移动执法终端，负责终端注册、终端登录、管控策略解析执行及结果上报、终端信息采集上报、状态监测、安全事件监测上报、模式切换上报等功能。

移动执法终端管理服务器负责终端管控策略的制订、下发及结果展示，终端信息和安全事件的汇总展现等功能。保证移动警务应用平稳过渡，满足移动办公、移动执法 APP 正常运行。

4.1.1 模式切换

根据移动执法终端的使用场景不同，移动执法终端管控系统提供个人模式、办公模式和监管区模式三种模式。可以通过管控后台、NFC 读卡器、及手动切换模式。

4.1.1.1 个人模式

个人模式为个人正常使用模式，为弱管控模式；

该模式下无法私自升级系统、刷机。可远程进行终端定位。

该模式下终端可以接入互联网；

个人模式下可安装使用互联网应用市场下的合法软件；

个人模式下电话通讯都可正常使用，其他终端功能均可正常使用。

4.1.1.2 办公模式

办公模式为中等管控模式，用于在监管区外进行移动办公；

该模式下支持网络访问黑白名单，屏蔽 WIFI 和蓝牙，禁用截屏、录屏功能；

该模式下终端接入移动执法专网；

办公模式下支持专有应用市场，移动办公类 APP 通过专有应用市场推送安装，个人不能任意下载安装 APP，其它模式的 APP 不能使用，不能浏览非指定链接；

办公模式下电话通讯都可正常使用；

该模式下强制设置登录密码。

4.1.1.3 监管区模式

监管区模式为强管控模式，用于民警在监管区内连接上移动执法专网使用；

该模式下不能调取系统设置、照相机、计算器等系统自带应用，屏蔽 WIFI 和蓝牙，禁用截屏、录屏功能。

该模式下支持专有应用市场，所使用移动执法类 APP 通过专有应用市场推送安装，个人不能任意下载安装 APP，其它模式的 APP 不能使用，不能浏览非指定链接；

该模式下不能连接除监管区移动执法专网外其它任何网络；

监管区模式下可以与全局移动执法终端和局内固话通讯，不能主动拨打外部电话，只能接听指定号码的拨入电话；

4.1.1.4 模式切换方式

个人模式和办公模式之间切换采用自主手动切换方式；

个人模式、办公模式切换到监管区模式：采用移动执法终端 NFC 读卡功能切换，终端通过刷监管区大门进口处安装的 NFC 设备，经过身份验证通过后，由个人模式或办公模式切换至监管区模式；

监管区模式切换到个人模式、办公模式：采用移动执法终端 NFC 读卡功能切换，终端通过刷监管区大门出口处安装的 NFC 设备，经身份验证通过后，由监管区模式切换至个人模式或办公模式；

移动执法终端管控系统可以通过后台远程对所有终端进行强制模式切换；

4.1.1.4 监管区模式切换显示

监管区大门出入口配置显示大屏，用于显示和播报终端个人模式和监管区模式切换信息，用于大门安检人员进行人工核验。

4.1.2 数据管理

移动执法终端在管控系统下数据分为两个域；

个人模式与其他两个模式数据安全隔离，文件系统、网络连接、外围设备接口、用户数据都彼此隔离，不能相互访问；

办公模式与监管区模式数据在可控下交互；

办公室模式和监管区模式应支持应用软件关闭后及时清除缓存页面、临时文件等剩余信息；

办公模式与监管区模式下禁止向 SIM 卡中写入数据；

4.1.3 终端安全管控能力

移动执法终端注册前，在管控后台建设终端配置库，并通过人、机、卡三码绑定方式实现终端的安全准入；

提供终端、SIM 卡分离自动锁定终端服务，可由管理员核对后进行解锁。

提供对应用程序的运行保护、安全隔离、数据防泄漏等必要保护措施。

提供移动执法终端截屏功能、网络共享功能、网络访问规则、锁屏密码方式、时间设置功能、恢复出厂功能、开发调试模式、系统升级功能、应用交互安装/卸载接口、应用静默安装/卸载接口与应用方式安装/卸载功能控制能力，实现终端基本功能按需使用目标。

提供移动执法终端对终端外设的管控，禁止/允许无线网络接入、开启蓝牙、使用定位服务、开启红外、USB 数据传输与调试、SD 卡存储、麦克风、摄像头、 NFC、生物特征识别模块、定位服务、扬声器、闪光灯与扩展外设控制的能力，实现终端外设按需使用目标。

提供移动执法终端接收到擦除数据策略时，应立即对终端进行数据擦除操作。

提供移动执法终端能够识别用户模式，并根据模式对终端网络参数进行配置。

提供移动执法终端定期检测终端的操作系统版本、SIM/USIM 卡、ROOT 状态，如发现变更，则进行提示、告警及合规管控处理，并作为安全事件上报。

提供移动执法终端支持终端 ROOT 监测功能，终端被 ROOT 后上报后台。

提供移动执法终端未经许可更换 SIM 卡后，可自动上报后台。

提供移动执法终端在注册后的预定期限内未进行登录时，终端安全监控组件应判定该终端为失联状态,自动执行合规管控处理(包括但不限于锁定终端、关闭终端、擦除数据等)，预定期限可配置，并随管控策略进行下发更新。

提供移动执法终端上报指定应用在指定时间间隔内消耗的网络流量、在前台的运行时间、使用频次。

提供移动执法终端上报终端硬件信息的功能，硬件信息包含但不限于终端厂商、终端型号、CPU 型号、运行内存容量、内部存储容量、屏幕分辨率、支持的移动网络制式等。

支持上报终端当前运行状态信息的功能，当前运行状态信息包含但不限于 CPU 使用率、内存使用率、存储使用率等。

提供终端锁定/解锁、数据擦除、终端重启、终端关机、定位信息上报、网络配置推送能力。

支持基于时间围栏、地理围栏的策略维护和自动触发机制。

支持对策略进行控制规则的管理，支持策略的继承、手工指定、策略覆盖、策略合并能力。

支持办公模式和监管区模式安全水印功能，防止偷拍屏幕造成信息泄露，同时支持防截屏、防录屏。

4.1.4 应用市场管理

办公模式和监管区模式下分别设置不同的应用市场程序；

支持应用远程分发、安装和卸载；支持应用的上架与下架管理，具备完善的审核机制；

支持应用标签化分类，方便管理与使用；

支持应用红/白/黑名单安装功能，对终端上未安装的红名单应用进行自动下载及后台静默安装，仅允许白名单应用列表中的应用安装，不允许黑名单应用列表中的应用安装。对移动执法终端上的黑名单列表中的应用阻止运行，支持进行后台静默卸载。

支持移动执法终端禁止卸载列表中的应用被卸载；

提供应用运行信息上报服务，包括但不仅限于移动执法专网联通监测、应用的使用情况，包括时长、流量、报错信息等。

4.1.5 信息推送

移动执法终端管控系统可向三种模式下的终端推送消息；

可通过定制向个人模式下终端跨域推送办公模式或监管区模式下应用系统生成的指定消息；

4.1.6 通讯功能

移动执法终端管控系统可以控制终端的通话功能的使用，可根据使用的具体需求，支持禁用和开通终端的通话和短信功能。

4.1.6.1 通话白名单

在监管区模式时，终端可以拨打和接听全局的移动执法终端号码和固话号码；

白名单由管控系统统一管理，可根据实际需要对不同用户进行配置和策略下发。

管控系统推送的白名单内的电话，只能接听不能主动拨打。

4.1.6.2 通话黑名单

终端可以设置通话黑名单，终端不能够接听和拨打黑名单之内的电话。

4.1.7 日志管理

移动执法终端管理系统提供完整日志管理功能，包括：管理员日志、终端日志、应用日志、调试日志。

提供报表功能：对移动执法终端的配置情况、应用的使用情况等各方面的统计分析日志。

对系统操作日志能够进行统一监测、采集及存储；并提供统一的系统日志搜索、查询等功能。

4.1.8 终端管理可视化

提供终端可视化管理界面，方便可视化指挥调度，可查看终端实时定位及历史轨迹。实现全面定位功能。便于第一时间精确定位执法终端的地理位置和出行路线，其中涉及个人非工作时间轨迹，由最高管理权限控制开启和关闭。

提供显示移动执法终端使用状态、应用流量排行、应用活跃度排行，及终端分布情况界面。

4.2 移动执法终端全生命周期管理系统

提供移动执法终端全生命周期管理系统，可按照单位集体管理和部署执法终端使用权限，也可根据个人特殊情况进行管理功能。

系统通过与移动执法终端管控系统进行数据对接，能够显示终端使用状态（正在使用、未使用、损害、丢失、状态变更时间、状态变更审批等）及相关信息（使用人、单位、部门、终端号码、所在模式、切换模式时间、APP 安装及使用情况等）。

实现内部人员组织关系调动：人员信息调动的每一条记录管理可查（例：人员调动 A 点 > B 点 > C 点 > A 点，时间节点全记录）；

实现外部调入：绑定终端记录（例：新终端启用；流转终端启用终端归属来源）；

实现调出外部：人员信息做特殊管理记录可查，终端流向管理标识，终端随同调出或解绑归还，归还入库管理记录等；

实现终端更换、丢失、维修记录：因何原因需要更换终端，旧终端信息和新终端信息及替换终端来源等，屏幕或主板（原主板串号，新主板串号）等维修信息管理记录；

实现人员离职、退休、调出或其他等：人员信息管理记录可查，终端随同调出或解绑归还，终端归还入库管理记录等；

实现终端记录：解绑未启用终端库存记录管理，管理记录终端来源、资产归属、存放地等，终端再次启用后库存记录跟随并入新绑定人员信息；

实现人员信息管理区分：可通过表或标识等区分在网人员与不在网人员（离职、退休、调出、其他等）信息，便于查询管理；

实现系统入职人员和启用弃用终端所有信息记录可管理查询；

实现管理平台数据（例：单位部门、日/周/月/年、切换模式人数/次数、当前各模式数量、各模式使用率占比、按单位部门模式使用率等）通过平台页面条件点选、筛选等一键生成报表，直观展示统计数据并可生成导出数据报表，能够实时查看掌握移动执法终端当前

及历史使用情况。

4.3 移动执法终端预置安装服务

4.3.1 预置安装移动执法终端安全监控组件服务

提供的移动执法终端预置移动执法终端安全监控组件服务，并对服务进行保活。

安全监控组件运行于移动警务执法终端，负责终端注册、终端登录、管控策略解析执行及结果上报、终端信息采集上报、安全事件监测上报、模式切换上报等功能。

4.3.2 预置安装移动警务门户服务

提供的移动执法终端预置移动警务门户服务、并对服务进行保活。

要求所提供的移动终端上预置移动警务门户，门户中包含：即时消息服务、通讯录以及基于客户端的基础服务组件。要求在执法终端开通后即可使用以上服务内容。

民警在使用各类移动执法、移动办公应用之前，必须先进入移动警务门户，移动警务门户提供应用的统一展示和运行环境。

移动警务门户与第五部分移动执法网络安全管理中的统一身份认证服务和单点登录服务进行对接，保证身份认证过程的安全性和用户身份的合法性。

移动警务门户提供全局通讯录展示能力、查询等服务。

移动警务门户整合即时消息服务，在门户中可以实时进行消息接收、消息发送等服务。

整合统一推送服务，提供通知和消息的统一入口，在移动警务门户展示相关的应用推送的通知。

4.4 运维支撑服务

4.4.1 5G 移动执法专网服务

提供面向用户的 5G 移动执法专网网管界面，支持面向用户的专网自服务平台，实现移动执法专网定制化可视化服务；

提供面向用户的 5G 移动执法专网网络运行状态、网络指标展示、接入用户信息、登入登出时间、状态、IP 地址等详细信息；

4.4.2 移动执法链路传输服务

提供面向网络运维人员网络监控管理工具，为其提供相应的技术工具，实现网络拓扑结构、网络故障、网络性能、网络配置的实时监控，及时发现网络故障、流量异常，提高网络管理效率，确保网络的安全性和可靠性。具备网络监控告警通知等能力。

提供基于裸光纤的传输专网运行状态监控，并提供故障告警、性能数据、监控展示的集中化管理。

4.4.3 移动执法终端管控服务

提供实时监控接入终端的安全状况、网络连接情况，并实现对监测信息、报警信息、安全事件信息等数据的查询和统计，监控安全接入平台运行总体情况；用户监控，即登录状态、操作行为、访问资源等；异常监控，包括异常用户、流量、设备等信息；按时间段、应用系统、用户单位分析统计用户信息、流量信息、异常信息；及时生成网络流量信息的报表。

提供移动执法终端开户、SIM 开通、终端的激活、开通、安装、下发等开通注册服务；

提供移动执法终端日常 7×24 小时热线服务，负责移动执法终端日常维护、技术支撑、故障处理、服务升级等服务；

提供移动执法终端业务支撑报告，包含：周报、月报、年报、故障处理情况等服务；

5、语音流量通讯服务

5.1 语音通讯服务

提供每个号码每月全国范围内不少于 1000 分钟主叫语音通讯套餐； 全局内部通话时长不计入套餐范围;

5.2 数据流量服务

提供每个号码不少于 200G 的全国不限速数据流量和 100 条短信，监管区内移动执法专网产生的流量不计入套餐范围；

5.3 SIM 卡及号码服务

现有移动执法终端不换号平滑过渡或提供连续不低于 500 个号码的手机号段，提供公户和个人户的快速开卡业务办理；

5.4 内部通讯服务

提供固话、移动执法终端之间内部短号免费通话功能，通话时长不占用执法终端语音套餐；

5.5 音频彩铃

为每个号码提供防止干预司法“三个规定”的定制音频彩铃；

6、移动执法网络安全服务

基于国密标准规范，提供统一身份认证、单点登录、数字证书、传输加密等服务能力，与移动执法、移动办公多平台应用融合，整体业务数据进行加密通信保障，提供全网全终端的安全接入服务平台。

6.1 SIM 卡安全认证服务

提供基于 SIM 卡的以用户身份为中心可信鉴权认证服务；

所有的移动执法终端配备内置支持国密算法的安全芯片的 SIM 卡，具备 NFC 近场交互能力；

提供基于 SIM 卡的安全认证网关服务，具备全网络、多终端（移动终端、PC 等）、多形态的安全接入能力；

支持信源+信道的数据传输加密服务；

6.2 统一身份认证服务

提供用户的实名认证服务。对用户进行身份实名核验，确保用户身份的合法性。

支持对接，认证方式支持账号认证、证书认证、短信认证、指纹认证等多因子认证；

提供 APP、PC、WEB 等多架构终端接入；

支持合规安全的国密 SIM 卡或 UKey 等多种认证介质；

支持单点登录，支持 CAS 协议，提供面向 Web 应用、C/S 应用、APP 应用等多种应用类型提供单点登录服务；

与移动警务门户服务集成，为移动警务门户提供的统一身份认证和应用单点登录的接口。

6.3 数据传输加密服务

提供端到端全流量 SSL 传输加密，保证重要信息数据的传输安全，规避公网传输业务数据被劫持解密的风险；

四、其它要求

4.1 合同签订

北京市外地罪犯遣送处与中标人签订合同并支付费用。

4.2 资产归属

中标人提供的所有用于服务的设备、器材、软件资产所有权归属中标人，服务期内使

用权归属甲方，中标人撤出设备须征得甲方同意。

4.3 保密要求

投标人应严格遵守国家和北京市政府的相关保密规定，认真履行保密义务，防止失密、窃密事件的发生。

投标人应承担对本项目内容的保密义务，未经采购人同意，不得公开或对外泄露任何信息。

中标人须与采购人签订保密协议。

4.4 交付及验收

中标人应在交付前完成移动警务采购项目各项功能的安装和调试工作，并在执法终端送达采购人指定地点后，由采购人和中标人按照执法终端数量的百分之五进行抽检。对执法终端产品规格、数量、包装、外观进行检查。同时对移动执法 5G 专网使用、光纤传输链路及网络传输设备配备开通情况、移动警务管控平台功能、语音流量通讯套餐、移动执法网络安全功能等进行查验，如发现产品存在问题或缺陷，采购人有权拒收并要求及时更换和调整。由此产生的后果，由中标人承担责任。

服务期结束前，采购人对中标人服务质量组织评价验收。各分合同单位如果购买金额不超当年《北京市政府采购集中采购目录及标准》分散采购限额的，由各分合同单位通过外请专家对中标人提供的服务进行评价验收，评价合格后各分合同单位可与中标人续签不超过 12 个月的服务合同；购买金额达到或超过当年《北京市政府采购集中采购目录及标准》分散采购限额的，按照政府采购相关规定执行项目采购。