# 北京市政府采购项目
# 竞争性磋商文件

项目名称：市局 2026 年购买移动警务服务项目

项目编号：0610-2641NF051066

采 购 人：北京市公安局

采购代理机构：北京国际招标有限公司

# 目　　录



注：采购文件条款中以“■”形式标记的内容适用于本项目，以“□”形式标记的内容不适用于本项目。

# 第一章　采购邀请

## 一、项目基本情况

1.项目编号：0610-2641NF051066

2.项目名称：市局 2026 年购买移动警务服务项目

3.采购方式：竞争性磋商

4.项目预算金额：47361.888 万元、项目最高限价（如有）：47361.888 万元

5.采购需求：市局 2026 年购买移动警务服务项目。本项目采购需求的详细内容见竞争性磋商文件第四章《采购需求》。

6.合同履行期限：3 年

7.本项目是否接受联合体：□是　■否。

## 二、申请人的资格要求（须同时满足）

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：

2.1 中小企业政策

■本项目不专门面向中小企业预留采购份额。

□本项目专门面向　□中小 □小微企业　采购。即：提供的货物全部由符合政策要求的中小企业制造、服务全部由符合政策要求的中小企业承接。

□本项目预留部分采购项目预算专门面向中小企业采购。对于预留份额，提供的货物由符合政策要求的中小企业制造、服务由符合政策要求的中小企业承接。预留份额通过以下措施进行：_____。

2.2 其它落实政府采购政策的资格要求：

（1）供应商未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

（2）凡受托为本次招标的项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动；

（3）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

3.本项目的特定资格要求：

3.1 本项目是否接受分支机构响应：■是；

3.2 本项目是否属于政府购买服务：

□否

■是，公益一类事业单位、使用事业编制且由财政拨款保障的群团组织，不得作为承接主体；

3.2 其他特定资格要求：供应商具备有效的中华人民共和国基础电信业务经营许可证。

**三、获取采购文件**

1.时间：2026 年 6 月 13 日至 2026 年 6 月 22 日，每天上午 9:00 至 11:30，下午 1:00 至 5:00（北京时间，法定节假日除外）。

2.地点：北京市政府采购电子交易平台

3.方式：供应商使用 CA 数字证书或电子营业执照登录北京市政府采购电子交易平台（http://zbcg-bjzc.zhongcy.com/bjczj-portal-site/index.html#/home）获取电子版竞争性磋商文件。

4.售价：0 元。

**四、响应文件提交**

截止时间：2026 年 6 月 23 日 9 点 30 分（北京时间）。

地点：北京市海淀区北三环中路 31 号院凯奇大厦 B 座 9 层 905 会议室。

**递交资料：**响应文件：正本：1 份、副本：5 份、电子版 1 份（须为正本的扫描件，以 U 盘形式并单独密封递交）以及单独密封的磋商保证金声明、报价一览表。

**五、开启**

时间：2026 年 6 月 23 日 9 点 30 分（北京时间）。

地点：北京市海淀区北三环中路 31 号院凯奇大厦 B 座 9 层 905 会议室。

**六、公告期限**

自本公告发布之日起 3 个工作日。

## 七、其他补充事宜

1.本项目需要落实的政府采购政策：本项目将严格落实节约能源、保护环境、扶持不发达地区和少数民族地区、促进中小企业发展及监狱企业发展、促进残疾人就业、信用记录查询、落实平等对待内外资企业、政采贷、政府采购异常低价审查等政府采购政策。

2.本项目采用**线上线下相结合采购方式（请按竞争性磋商文件要求现场递交纸质响应文件）**，请供应商认真学习北京市政府采购电子交易平台发布的相关操作手册（供应商可在交易平台下载相关手册），办理 CA 数字证书或电子营业执照、进行北京市政府采购电子交易平台注册绑定，并认真核实 CA 数字证书或电子营业执照情况确认是否符合本项目电子化采购流程要求。

CA 数字证书服务热线 010-58511086

电子营业执照服务热线 400-699-7000

技术支持服务热线 010-86483801

2.1 办理 CA 数字证书或电子营业执照

供应商登录北京市政府采购电子交易平台查阅 “用户指南”—“操作指南”—“市场主体 CA 办理操作流程指引” /“电子营业执照使用指南”，按照程序要求办理。

2.2 注册

供应商登录北京市政府采购电子交易平台“用户指南”—“操作指南”—“市场主体注册入库操作流程指引”进行自助注册绑定。

2.3 驱动、客户端下载

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“招标采购系统文件驱动安装包”下载相关驱动。

供应商登录北京市政府采购电子交易平台“用户指南”—“工具下载”—“投标文件编制工具”下载相关客户端。

2.4 获取电子竞争性磋商文件

供应商使用 CA 数字证书或电子营业执照登录北京市政府采购电子交易平台获取电子竞争性磋商文件。

供应商如计划参与多个采购包的响应，应在登录北京市政府采购电子交易平台后，在【我的项目】栏目依次选择对应采购包，进入项目工作台招标/采购文件环节分别按采购包下载采购文件电子版。未在规定期限内按上述操作获取文件的响应无效。

**八、对本次采购提出询问，请按以下方式联系。**

**1.采购人信息**

名　　称：北京市公安局

地　　址：北京市东城区前门东大街 9 号

联系方式：孔警官 010-65223229

**2.采购代理机构信息**

名　　称：北京国际招标有限公司

地　　址：北京市海淀区北三环中路 31 号院凯奇大厦 B 座 9 层

联系方式：刘思雯 张鑫 010-84045310

**3.项目联系方式**

项目联系人：刘思雯 张鑫

电　　话：010-84045310

电子信箱：liusw@zgcgroup.com.cn

开户名（全称）：北京国际招标有限公司

开户银行：华夏银行建国门支行

账　　号：10265000000524102

# 第二章　供应商须知

## 供应商须知资料表

本表是对供应商须知的具体补充和修改，如有矛盾，均以本资料表为准。

<table>
<tr><th>条款号</th><th>条目</th><th>内容</th></tr>
<tr><td>2.2</td><td>项目属性</td><td>项目属性：<br>■服务<br>□货物<br>□工程</td></tr>
<tr><td>2.3</td><td>科研仪器设备</td><td>是否属于科研仪器设备采购项目：<br>□是<br>■否</td></tr>
<tr><td rowspan="2">3.1</td><td>现场考察</td><td>■不组织<br>□组织，考察时间：___年___月___日___点___分<br>考察地点：_____。</td></tr>
<tr><td>磋商前答疑会</td><td>■不召开<br>□召开，召开时间：___年___月___日___点___分<br>召开地点：_____。</td></tr>
<tr><td>4.2.5</td><td>标的所属行业</td><td>本项目采购标的对应的中小企业划分标准所属行业：<br><table><tr><td>标的名称</td><td>中小企业划分标准所属行业</td></tr><tr><td>市局 2026 年购买移动警务服务项目</td><td>信息传输业</td></tr></table></td></tr>
<tr><td>10.2</td><td>报价</td><td>报价的特殊规定：<br>■无<br>□有，具体情形：____。</td></tr>
<tr><td>11.1</td><td rowspan="2">磋商保证金</td><td>磋商保证金金额：人民币捌拾万元整（¥800,000.00）<br>磋商保证金收受人信息：<br>开户名（全称）：北京国际招标有限公司<br>开户银行：华夏银行北京建国门支行<br>账　　号：10265000000524102<br>磋商保证金递交时间：响应文件提交截止期前（2026 年 6 月 23 日 9 点 30 分）<br>汇款备注：2641NF051066 保证金<br>供应商未按照竞争性磋商文件要求提交磋商保证金的，响应无效。</td></tr>
<tr><td>11.8.5</td><td>磋商保证金不予退还的其他情形：<br>■无<br>□有，具体情形：_____。</td></tr>
<tr><td>12.1</td><td>响应有效期</td><td>自响应文件提交截止之日起算 90 日历天。</td></tr>
<tr><td>20.1</td><td>确定成交供应</td><td>采购人是否授权磋商小组直接确定成交供应商：</td></tr>
</table>

<table>
<tr><th>条款号</th><th>条目</th><th>内容</th></tr>
<tr><td></td><td>商</td><td>■否<br>□是<br>成交候选人并列的，按照以下方式确定成交供应商：<br>■得分且最终报价均相同的，以供应商“技术部分”得分高者为成交供应商。<br>□随机抽取。</td></tr>
<tr><td>23.5</td><td>分包</td><td>本项目是否允许分包：<br>■不允许<br>□允许，具体要求：_____。<br>（1）可以分包履行的具体内容：_____；<br>（2）允许分包的金额或者比例：_____；<br>（3）其他要求：_____。</td></tr>
<tr><td>23.6</td><td>政采贷</td><td>为更大力度激发市场活力和社会创造力，增强发展动力，按照《北京市全面优化营商环境助力企业高质量发展实施方案》（京政办发〔2023〕8 号）部署，进一步加强政府采购合同线上融资“一站式” 服务（以下简称“政采贷”），北京市财政局、中国人民银行营业管 理部联合发布《关于推进政府采购合同线上融资有关工作的通知》（京财采购〔2023〕637 号）。有需求的供应商，可按上述通知要求办理“政采贷”。</td></tr>
<tr><td>24.1.1</td><td>询问</td><td>询问提出形式：电话或书面方式。</td></tr>
<tr><td>24.3</td><td>联系方式</td><td>接收询问和质疑的联系方式<br>联系部门：北京国际招标有限公司 业务五部；<br>联系电话：010-84045310；<br>通讯地址：北京市海淀区北三环中路 31 号院凯奇大厦 B 座 9 层 906。</td></tr>
<tr><td>25</td><td>代理费</td><td>收费对象：<br>□采购人<br>■成交供应商<br>收费标准：按照成交金额依据以下规定的成交代理服务收费标准（服务），按差额定律累进法的标准计算后下浮 20%向成交供应商收取成交服务费用。
<table>
<tr><th>服务类型<br>费率<br>中标金额（万元）</th><th>货物招标</th><th>服务招标</th><th>工程招标</th></tr>
<tr><td>100 以下</td><td>1.5%</td><td>1.5%</td><td>1.0%</td></tr>
<tr><td>100-500</td><td>1.1%</td><td>0.8%</td><td>0.7%</td></tr>
<tr><td>500-1000</td><td>0.8%</td><td>0.45%</td><td>0.55%</td></tr>
<tr><td>1000-5000</td><td>0.5%</td><td>0.25%</td><td>0.35%</td></tr>
<tr><td>5000-10000</td><td>0.25%</td><td>0.1%</td><td>0.2%</td></tr>
<tr><td>10000-100000</td><td>0.05%</td><td>0.05%</td><td>0.05%</td></tr>
<tr><td>1000000 以上</td><td>0.01%</td><td>0.01%</td><td>0.01%</td></tr>
</table>
例：成交金额为 200 万元，计算成交代理服务费额如下：<br>100 万元×1.5%=1.5 万元<br>（200-100）万元×0.8%=0.8 万元<br>合计收费=（1.5 万元+0.8 万元）×80%=1.84 万元<br>缴纳时间：在收到成交通知书后按竞争性磋商文件的规定缴纳。</td></tr>
</table>

# 供应商须知

## 一　说　明

1　采购人、采购代理机构、供应商、联合体

1.1　采购人、采购代理机构：指依法进行政府采购的国家机关、事业单位、团体组织，及其委托的采购代理机构。本项目采购人、采购代理机构见第一章《采购邀请》。

1.2　供应商（也称“申请人”）：指向采购人提供货物、工程或者服务的法人、其他组织或者自然人。

1.3　联合体：指两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购。

2　资金来源、项目属性、科研仪器设备采购

2.1　资金来源为财政性资金和/或本项目采购中无法与财政性资金分割的非财政性资金。

2.2　项目属性见《供应商须知资料表》。

2.3　是否属于科研仪器设备采购见《供应商须知资料表》。

3　现场考察、磋商前答疑会

3.1　若《供应商须知资料表》中规定了组织现场考察、召开磋商前答疑会，则供应商应按要求在规定的时间和地点参加。

3.2　由于未参加现场考察或磋商前答疑会而导致对项目实际情况不了解，影响响应文件编制、报价准确性、综合因素响应不全面等问题的，由供应商自行承担不利评审后果。

4　政府采购政策（包括但不限于下列具体政策要求）

4.1　采购本国货物、工程和服务

4.1.1　政府采购应当采购本国货物、工程和服务。但有《**中华人民共和国政府采购法**》第十条规定情形的除外。

4.1.2　本项目如接受非本国货物、工程、服务参与响应，则具体要求见第四章《采购需求》。

4.1.3　进口产品指通过中国海关报关验放进入中国境内且产自关境外的产品，包括已经进入中国境内的进口产品。关于进口产品的相关规定依

据《政府采购进口产品管理办法》（财库〔2007〕119 号文）、《关于政府采购进口产品管理有关问题的通知》（财办库〔2008〕248 号文）。

4.2 本国产品

本项目按照《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）和《关于贯彻落实<国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知>的意见》（财库〔2025〕30 号）有关要求，落实本国产品标准。

4.3 中小企业、监狱企业及残疾人福利性单位

4.3.1 中小企业定义：

4.3.1.1 中小企业是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。关于中小企业的判定依据《中华人民共和国中小企业促进法》、《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）、《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）、《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300 号）、《金融业企业划型标准规定》（银发〔2015〕309 号）等国务院批准的中小企业划分标准执行。

4.3.1.2 供应商提供的货物、工程或者服务符合下列情形的，享受中小企业扶持政策：

（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；

（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；

（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订

立劳动合同的从业人员。

4.3.1.3 在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受中小企业扶持政策。

4.3.1.4 以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

4.3.2 在政府采购活动中，监狱企业视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。监狱企业定义：是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地（设区的市）监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。

4.3.3 在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等促进中小企业发展的政府采购政策。残疾人福利性单位定义：享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

4.3.3.1 安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；

4.3.3.2 依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

4.3.3.3 为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

4.3.3.4 通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

4.3.3.5 提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）；

4.3.3.6 前款所称残疾人是指法定劳动年龄内，持有《中华人民共和

国残疾人证》或者《中华人民共和国残疾军人证（1 至 8 级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或服务协议的雇员人数。

4.3.4 本项目是否专门面向中小企业预留采购份额见第一章《采购邀请》。

4.3.5 采购标的对应的中小企业划分标准所属行业见《供应商须知资料表》。

4.3.6 小微企业价格评审优惠的政策调整：见第三章《评审方法和评审标准》。

4.4 政府采购节能产品、环境标志产品

4.4.1 政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门根据产品节能环保性能、技术水平和市场成熟程度等因素，确定实施政府优先采购和强制采购的产品类别及所依据的相关标准规范，以品目清单的形式发布并适时调整。依据品目清单和认证证书实施政府优先采购和强制采购。

4.4.2 采购人拟采购的产品属于品目清单范围的，采购人及其委托的采购代理机构依据国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，对获得证书的产品实施政府优先采购或强制采购。关于政府采购节能产品、环境标志产品的相关规定依据《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）。

4.4.3 如本项目采购产品属于实施政府强制采购品目清单范围的节能产品，则供应商所报产品必须获得国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则**响应无效**；

4.4.4 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施政府优先采购。优先采购的具体规定见第三章《评审方法和评审标准》（如涉及）。

4.5 正版软件

4.5.1 各级政府部门在购置计算机办公设备时，必须采购预装正版操作系统软件的计算机产品，相关规定依据《国家版权局、信息产业部、财政部、国务院机关事务管理局关于政府部门购置计算机办公设备必须采购已预装正版操作系统软件产品的通知》（国权联〔2006〕1 号）、

《国务院办公厅关于进一步做好政府机关使用正版软件工作的通知》（国办发〔2010〕47 号）、《财政部关于进一步做好政府机关使用正版软件工作的通知》（财预〔2010〕536 号）。

4.6 网络安全专用产品

4.6.1 根据《关于调整网络安全专用产品安全管理有关事项的公告》（2023 年第 1 号），所提供产品属于列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品时，应当按照《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求。

4.7 推广使用低挥发性有机化合物（VOCs）

4.7.1 为全面推进本市挥发性有机物（VOCs）治理，贯彻落实挥发性有机物污染治理专项行动有关要求，相关规定依据《北京市财政局北京市生态环境局关于政府采购推广使用低挥发性有机化合物（VOCs）有关事项的通知》（京财采购〔2020〕2381 号）。本项目中涉及涂料、胶黏剂、油墨、清洗剂等挥发性有机物产品的，属于强制性标准的，供应商应执行符合本市和国家的 VOCs 含量限制标准（具体标准见第四章《采购需求》），否则**响应无效**；属于推荐性标准的，优先采购，具体见第三章《评审方法和评审标准》。

4.8 采购需求标准

4.8.1 商品包装、快递包装政府采购需求标准（试行）

为助力打好污染防治攻坚战，推广使用绿色包装，根据财政部关于印发《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），本项目如涉及商品包装和快递包装的，则其具体要求见第四章《采购需求》。

4.8.2 其他政府采购需求标准

为贯彻落实《深化政府采购制度改革方案》有关要求，推动政府采购需求标准建设，财政部门会同有关部门制定发布的其他政府采购需求标准，本项目如涉及，则具体要求见第四章《采购需求》。

5 响应费用

5.1 供应商应自行承担所有与准备和参加磋商有关的费用，无论磋商的结果如何，

采购人或采购代理机构在任何情况下均无承担这些费用的义务和责任。

## 二　竞争性磋商文件

6　竞争性磋商文件构成

6.1　竞争性磋商文件包括以下部分：

第一章　采购邀请

第二章　供应商须知

第三章　评审方法和评审标准

第四章　采购需求

第五章　合同草案条款

第六章　响应文件格式

6.2　供应商应认真阅读竞争性磋商文件的全部内容。供应商应按照竞争性磋商文件要求提交响应文件并保证所提供的全部资料的真实性，并对竞争性磋商文件做出实质性响应，否则**响应无效**。

7　对竞争性磋商文件的澄清或修改

7.1　采购人、采购代理机构或者磋商小组对已发出的竞争性磋商文件进行必要澄清或者修改的，将以书面形式通知所有获取竞争性磋商文件的潜在供应商。采用公告方式邀请供应商参与的，还将在原公告发布媒体上发布更正公告。

7.2　上述书面通知，按照获取竞争性磋商文件的潜在供应商提供的联系方式发出，因提供的信息有误导致通知延迟或无法通知的，采购人或采购代理机构不承担责任。

7.3　澄清或者修改的内容为竞争性磋商文件的组成部分，并对所有获取竞争性磋商文件的潜在供应商具有约束力。澄清或者修改的内容可能影响响应文件编制的，将在提交首次响应文件截止之日 3 个工作日前，以书面形式通知所有获取磋商文件的供应商；不足上述时间的，将顺延提交首次响应文件截止时间。

## 三　响应文件的编制

8　响应范围、竞争性磋商文件中计量单位的使用及磋商语言

8.1 本项目如划分采购包，供应商可以对本项目的其中一个采购包进行响应，也可同时对多个采购包进行响应。供应商应当对所参与采购包对应第四章《采购需求》所列的全部内容进行响应，不得将一个采购包中的内容拆分响应，否则其对该采购包的响应将被认定为**无效响应**。

8.2 除竞争性磋商文件有特殊要求外，本项目磋商所使用的计量单位，应采用中华人民共和国法定计量单位。

8.3 除专用术语外，响应文件及来往函电均应使用中文书写。必要时专用术语应附有中文解释。供应商提交的支持资料和已印制的文献可以用外文，但相应内容应附有中文翻译本，在解释响应文件时以中文翻译本为准。未附中文翻译本或翻译本中文内容明显与外文内容不一致的，其不利后果由供应商自行承担。

9 响应文件构成

9.1 供应商应当按照竞争性磋商文件的要求编制响应文件，并对其提交的响应文件的真实性、合法性承担法律责任。响应文件的部分格式要求，见第六章《响应文件格式》。

9.2 对于竞争性磋商文件中标记了“实质性格式”文件的，供应商不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，**否则响应无效**。未标记“实质性格式”的文件和竞争性磋商文件未提供格式的内容，可由供应商自行编写。

9.3 第三章《评审方法和评审标准》中涉及的证明文件。

9.4 对照第四章《采购需求》，说明所提供货物和服务已对第四章《采购需求》做出了响应，或申明与第四章《采购需求》的偏差和例外。如第四章《采购需求》中要求提供证明文件的，供应商应当按具体要求提供证明文件。

9.5 供应商认为应附的其他材料。

10 报价

10.1 所有响应均以人民币为计价货币。

10.2 供应商的报价应包括为完成本项目所发生的一切费用和税费，采购人将不再支付报价以外的任何费用。供应商的报价应包括但不限于下列内容，《供应商须知资料表》中有特殊规定的，从其规定。

10.2.1 响应货物及标准附件、备品备件、专用工具等的出厂价（包括已在中国国内的进口货物完税后的仓库交货价、展室交货价或货架交货价）和运至最终目的地的运输费和保险费，安装调试、检验、技术服务、培训、质量保证、售后服务、税费等；

10.2.2 按照竞争性磋商文件要求完成本项目的全部相关费用。

10.3 采购人不得向供应商索要或者接受其给予的赠品、回扣或者与采购无关的其他商品、服务。

10.4 供应商不能提供任何有选择性或可调整的最后报价（竞争性磋商文件另有规定的除外），否则其**响应无效**。

11 磋商保证金

11.1 供应商应按《供应商须知资料表》中规定的金额及要求交纳磋商保证金。供应商自愿超额缴纳磋商保证金的，响应文件不做无效处理。

11.2 交纳磋商保证金可采用的形式：政府采购法律法规接受的支票、汇票、本票、网上银行支付或者金融机构、担保机构出具的保函等非现金形式。

11.3 磋商保证金到账（保函提交）截止时间同首次响应文件提交截止时间。以支票、汇票、本票、网上银行支付等形式提交磋商保证金的，应在首次响应文件提交截止时间前到账；以金融机构、担保机构出具的纸质保函等形式提交磋商保证金的，应在首次响应文件提交截止时间前将原件提交至采购代理机构；以电子保函形式提交磋商保证金的，应在首次响应文件提交截止时间前通过北京市政府采购电子交易平台完成电子保函在线办理。未按上述要求缴纳保证金的，其**响应无效**。

11.4 供应商需在响应文件中提供“磋商保证金凭证/交款单据复印件”。

11.5 磋商保证金有效期同响应有效期。

11.6 供应商为联合体的，可以由联合体中的一方或者多方共同交纳磋商保证金，其交纳的保证金对联合体各方均具有约束力。

11.7 采购人、采购代理机构将及时退还供应商的保证金，采用银行保函、担保机构担保函等形式递交的保证金，经供应商同意后采购人、采购代理机构可以不再退还，但因供应商自身原因导致无法及时退还的除外：

11.7.1 已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。采购人、采购代理机构将退还退出磋商的供应商的磋商保

证金；

11.7.2 成交供应商的磋商保证金，在采购合同签订后 5 个工作日内退还成交供应商；

11.7.3 未成交供应商的磋商保证金，在成交通知书发出后 5 个工作日内退还。

11.8 有下列情形之一的，采购人或采购代理机构不予退还磋商保证金：

11.8.1 供应商在响应文件提交截止时间后撤回响应文件的；

11.8.2 供应商在响应文件中提供虚假材料的；

11.8.3 除因不可抗力或磋商文件认可的情形以外，成交供应商不与采购人签订合同的；

11.8.4 供应商与采购人、其他供应商或者采购代理机构恶意串通的；

11.8.5 《供应商须知资料表》规定的其他情形。

12 响应有效期

12.1 响应文件应在本竞争性磋商文件《供应商须知资料表》中规定的响应有效期内保持有效，响应有效期少于竞争性磋商文件规定期限的，其**响应无效**。

13 响应文件的签署、盖章

13.1 供应商应准备响应文件**正本 1 份、副本 5 份、电子版 1 份**，每份响应文件须清楚地标明“正本”、“副本”或“电子版”字样。若正本和副本不符，以正本为准。

13.2 响应文件的正本需打印或用不退色墨水书写，并由供应商的法定代表人或经其正式授权的代表在响应文件上签字并加盖单位公章。授权代表须持有书面的“授权委托书”（标准格式附后），并将其附在响应文件中。如对响应文件进行了修改，则应由供应商的法定代表人或经其正式授权的代表在修改的每一页上签字或加盖供应商本单位公章。响应文件的副本可采用正本的复印件形式。响应文件的电子版内容为响应文件正本的扫描件。

13.3 响应文件因字迹潦草或表达不清所引起的后果由供应商负责。

13.4 任何行间插字、涂改和增删，必须由响应文件签字人签字或盖本单位公章后才有效。

13.5 响应文件建议采用胶装形式进行装订。

## 四　响应文件的提交

14 响应文件的提交

14.1　递交时，供应商应将响应文件正本和所有的副本以及电子版分开密封装在单独的密封袋中，且在密封袋正面标明“正本”“副本”“电子版”字。

14.2　为方便磋商，供应商应将“报价一览表”单独密封，并在信封上表明“报价一览表”字样，在递交文件时单独递交。

14.3　为方便核查保证金，供应商应将“保证金”单独密封，并在密封袋上表明“保证金”字样，在递交文件时单独递交。

14.4　所在密封袋上均应：

（1）清楚标明递交至响应文件中指明的地址。

（2）注明响应文件中指明的项目名称、项目编号和“在 （磋商日期、时间）之前不得启封”的字样。

（3）在密封袋的封装处加盖供应商公章。

14.5　如果供应商未按上述要求密封并加标记，采购人或采购代理机构对响应文件的误投或过早启封概不负责。

14.6　所有信封上还应写明供应商名称及地址，以便若其响应文件被宣布未“迟到”时，能原封退回。

15 响应文件提交截止时间

15.1　供应商应在磋商公告或磋商邀请书中规定的截止日期和时间前，将响应文件密封递交，递交地点应是磋商公告或磋商邀请书中规定的地址。

15.2　在截止时间后送达的响应文件，采购人、采购代理机构或者磋商小组将拒收。

16 响应文件的修改与撤回

16.1　供应商对响应文件的补充、修改的内容应当按照竞争性磋商文件要求签署、盖章，作为响应文件的组成部分。补充、修改的内容与响应文件不一致的，以补充、修改的内容为准。供应商对响应文件的修改和撤回通知应按本须知规定编制、密封、标记和发送。

16.2　响应文件提交截止时间前，供应商可以对响应文件进行补充、修改或者撤回。

## 五　评审

17 组织磋商

17.1 采购人或采购代理机构将按竞争性磋商文件的规定，在响应文件提交截止时间的同一时间和竞争性磋商文件预先确定的地点开启响应文件。

17.2 供应商认为采购人员及相关人员与其他供应商有利害关系的，可以向采购人或采购代理机构书面提出回避申请，并说明理由。采购人或采购代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员将回避。

17.3 供应商不足 3 家的，不予开启响应文件。

17.4 本项目不公开报价。

18 磋商小组

18.1 磋商小组根据政府采购有关规定和本次采购项目的特点进行组建，并负责具体评审与磋商事务，独立履行职责。

18.2 评审专家须符合《财政部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）的规定。依法自行选定评审专家的，采购人和采购代理机构将查询有关信用记录，对具有行贿、受贿、欺诈等不良信用记录的人员，拒绝其参与政府采购活动。

19 评审方法和评审标准

19.1 见第三章《评审方法和评审标准》。

## 六 确定成交

20 确定成交供应商

20.1 采购人将在收到评审报告后，从评审报告提出的成交候选供应商中，按照排序由高到低的原则确定成交供应商。采购人是否授权磋商小组直接确定成交供应商，见《供应商须知资料表》。成交候选人并列的，按照《供应商须知资料表》要求确定成交供应商。

21 成交公告与成交通知书

21.1 采购人或采购代理机构将在成交供应商确定后 2 个工作日内，在北京市政府采购网公告成交结果，同时向成交供应商发出成交通知书，成交公告期限为 1 个工作日。

21.2 成交通知书对采购人和成交供应商均具有法律效力。成交通知书发出后，采购人改变成交结果的，或者成交供应商放弃成交项目的，应当依法承担法律责任。

22 终止

22.1 出现下列情形之一的，采购人或采购代理机构将终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

22.1.1 因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；

22.1.2 出现影响采购公正的违法、违规行为的；

22.1.3 除了“市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目，提交最后报价的供应商可以为 2 家；政府购买服务项目（含政府和社会资本合作项目），在采购过程中符合要求的供应商（社会资本）只有 2 家的，竞争性磋商采购活动可以继续进行”的情形外，在采购过程中符合要求的供应商或者报价未超过采购预算的供应商不足 3 家的。

23 签订合同

23.1 采购人与成交供应商应当在成交通知书发出之日起 30 日内，按照磋商文件确定的合同文本以及采购标的、规格型号、采购金额、采购数量、技术和服务要求等事项签订政府采购合同。

23.2 成交供应商拒绝签订政府采购合同的，采购人可以按照评审报告推荐的成交候选人名单排序，确定下一候选人为成交供应商，也可以重新开展采购活动。拒绝签订政府采购合同的成交供应商不得参加对该项目重新开展的采购活动。

23.3 联合体成交的，联合体各方应当共同与采购人签订合同，就采购合同约定的事项向采购人承担连带责任。

23.4 政府采购合同不能转包。

23.5 采购人允许采用分包方式履行合同的，成交供应商可以依法采取分包方式履行合同。本项目是否允许分包，见《供应商须知资料表》。政府采购合同分包履行的，应当在响应文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包，**否则响应无效**。成交供应商就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

23.6 “政采贷”融资指引：详见《供应商须知资料表》。

24 询问与质疑

24.1 询问

24.1.1 供应商对政府采购活动事项有疑问的，可依法向采购人或采购代理机

构提出询问，提出形式见《供应商须知资料表》。

24.1.2 采购人或采购代理机构对供应商依法提出的询问，在 3 个工作日内作出答复，但答复的内容不得涉及商业秘密。

24.2 质疑

24.2.1 供应商认为竞争性磋商文件、采购过程、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起 7 个工作日内，以书面形式向采购人、采购代理机构提出质疑。采购人、采购代理机构在收到质疑函后 7 个工作日内作出答复。

24.2.2 质疑函须使用财政部制定的范本文件。供应商为自然人的，质疑函应当由本人签字；供应商为法人或者其他组织的，质疑函应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

24.2.3 供应商委托代理人进行质疑的，应当随质疑函同时提交供应商签署的授权委托书。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

24.2.4 供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑，法定质疑期内针对同一采购程序环节再次提出的质疑，采购人、采购代理机构有权不予答复。

24.3 接收询问和质疑的联系部门、联系电话和通讯地址见《供应商须知资料表》。

25 代理费

25.1 收费对象、收费标准及缴纳时间见《供应商须知资料表》。由成交供应商支付的，成交供应商须一次性向采购代理机构缴纳代理费，报价应包含代理费用。

# 第三章　评审方法和评审标准

## 一、评审程序和方法

1　响应文件的资格审查和符合性审查

1.1　磋商小组将根据《资格审查要求》和《符合性审查要求》中规定的内容，对供应商进行检查，并形成检查结果。供应商《响应文件》有任何一项不符合《资格审查要求》和《符合性审查要求》要求的，视为未实质性响应磋商文件。未实质性响应磋商文件的响应文件按**无效响应**处理，磋商小组应当告知提交响应文件的供应商。

1.2　《资格审查要求》中对格式有要求的，除竞争性磋商文件另有规定外，均为“实质性格式”文件。

1.3　《资格审查要求》见下表：

**资格审查要求**

| 序号 | 检查因素 | 检查内容 | 格式要求 |
|---|---|---|---|
| 1 | 满足《中华人民共和国政府采购法》第二十二条规定 | 具体规定见第一章《采购邀请》 | |
| 1-1 | 营业执照等证明文件 | 供应商为企业（包括合伙企业）的，应提供有效的“营业执照”；<br>供应商为事业单位的，应提供有效的“事业单位法人证书”；<br>供应商是非企业机构的，应提供有效的“执业许可证”、“登记证书”等证明文件；<br>供应商是个体工商户的，应提供有效的“个体工商户营业执照”；<br>供应商是自然人的，应提供有效的自然人身份证明。<br>分支机构参加响应的，应提供该分支机构或其所属法人/其他组织的相应证明文件；**同时**还应提供其所属法人/其他组织出具的授权其参与本项目的授权书（格式自拟，须加盖其所属法人/其他组织的公章）；对于银行、保险、石油石化、电力、电信等行业的分支机构，可以提供上述授权，也可以提供其所属法人/其他组织的有关文件或制度等能够证明授权其独立开展业务的证明材料。 | 提供证明文件的复印件并加盖公章 |

| 序号 | 检查因素 | 检查内容 | 格式要求 |
| --- | --- | --- | --- |
| 1-2 | 供应商资格声明书 | 提供了符合竞争性磋商文件要求的《供应商资格声明书》。 | 格式见《响应文件格式》 |
| 1-3 | 供应商信用记录 | 查询渠道：信用中国网站和中国政府采购网（www.creditchina.gov.cn、www.ccgp.gov.cn）；<br>截止时点：首次响应文件提交截止时间以后、资格审查阶段采购人或采购代理机构的实际查询时间；<br>信用信息查询记录和证据留存具体方式：查询结果网页打印页作为查询记录和证据，与其他竞争性磋商文件一并保存；<br>信用信息的使用原则：经认定的被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商，其**响应无效**。联合体形式磋商的，联合体成员存在不良信用记录，视同联合体存在不良信用记录。 | 无须供应商提供，由采购人或采购代理机构查询。 |
| 1-4 | 法律、行政法规规定的其他条件 | 法律、行政法规规定的其他条件 | / |
| 2 | 落实政府采购政策需满足的资格要求 | 具体要求见第一章《采购邀请》 | |
| 2-1 | 中小企业政策证明文件 | 具体要求见第一章《采购邀请》 | |
| 2-1-1 | 中小企业证明文件（**本项目不专门面向中小企业预留采购份额**） | 当本项目（包）涉及预留份额专门面向中小企业采购，提供如下资料：<br>1、供应商单独响应的，应提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。<br>2、如磋商文件要求以联合体形式参加或者要求合同分包的，且供应商为联合体或拟进行合同分包的，则联合体中的中小企业、签订分包意向协议的中小企业具体情况须在《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件中如实填报，且满足采购文件关于预留份额的要求。 | 格式见《响应文件格式》 |

| 序号 | 检查因素 | 检查内容 | 格式要求 |
| --- | --- | --- | --- |
| 2-1-2 | 拟分包情况说明及分包意向协议**（本项目不允许分包）** | 如本项目（包）要求通过分包措施预留部分采购份额面向中小企业采购、且供应商因落实政府采购政策拟进行分包的，必须提供；否则无须提供。<br>对于预留份额专门面向中小企业采购的项目（包），组成联合体或者接受分包合同的中小企业与联合体内其他企业、分包企业之间不得存在直接控股、管理关系。 | / |
| 2-2 | 其它落实政府采购政策的资格要求 | 如有，见第一章《采购邀请》 | 提供供应商资格声明书（格式），已提供过的不用重复提供。 |
| 3 | 本项目的特定资格要求 | 如有，见第一章《采购邀请》 | |
| 3-1 | 本项目对于联合体的要求**（本项目不接受联合体）** | 1、如本项目接受联合体磋商，且供应商为联合体时必须提供《联合协议》，明确各方拟承担的工作和责任，并指定联合体牵头人，授权其代表所有联合体成员负责本项目磋商和合同实施阶段的牵头、协调工作。该联合协议应当作为响应文件的组成部分，与响应文件其他内容同时提交。<br>2、联合体各成员单位均须提供本表中序号1-1、1-2 的证明文件。联合体各成员单位均应满足本表 3-2 项规定。<br>3、本表序号 3-3 项规定的其他特定资格要求中的每一小项要求，联合体各方中至少应当有一方符合本表中其他资格要求并提供证明文件。<br>4、联合体中有同类资质的供应商按照联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级。<br>5、以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。<br>6、若联合体中任一成员单位中途退出，则该联合体的**响应无效**。<br>**7、本项目不接受联合体响应时，供应商不得为联合体。** | / |

| 序号 | 检查因素 | 检查内容 | 格式要求 |
| --- | --- | --- | --- |
| 3-2 | 政府购买服务承接主体的要求（**本项目为政府购买服务项目**） | 如本项目属于政府购买服务，供应商不属于公益一类事业单位、使用事业编制且由财政拨款保障的群团组织。 | 格式见《响应文件格式》“1-2 供应商资格声明书” |
| 3-3 | 其他特定资格要求 | 供应商具备有效的中华人民共和国基础电信业务经营许可证。 | 提供证明文件的复印件并加盖公章 |
| 4 | 磋商保证金 | 按照竞争性磋商文件的要求提交磋商保证金。 | 磋商保证金凭证/交款单据复印件 |
| 5 | 获取磋商文件 | 在规定期限内通过北京市政府采购电子交易平台获取所参与包的磋商文件。<br>注：如本项目接受联合体，且供应商为联合体时，联合体中任一成员获取文件即视为满足要求。 | / |

1.4 《符合性审查要求》见下表：

**符合性审查要求**

| 序号 | 检查因素 | 检查内容 | 是否允许澄清、说明或者更正 |
| --- | --- | --- | --- |
| 1 | 授权委托书 | 按磋商文件要求提供授权委托书； | 否 |
| 2 | 响应完整性 | 未将一个采购包中的内容拆开响应； | 否 |
| 3 | 报价 | 报价未超过磋商文件中规定的项目预算金额或者项目最高限价； | 否 |
| 4 | 有效期 | 响应文件中承诺的有效期满足磋商文件中载明的有效期的； | 否 |
| 5 | 签署、盖章 | 按照磋商文件要求签署、盖章的； | 否 |
| 6 | 实质性格式 | 标记为“实质性格式”的文件均按磋商文件要求提供； | 否 |
| 7 | ★号条款响应 | 响应文件满足磋商文件第四章《采购需求》中★号条款要求的； | 否 |

| | | | |
|---|---|---|---|
| 8 | 公平竞争 | 供应商遵循公平竞争的原则，不存在恶意串通，妨碍其他供应商的竞争行为，不存在损害采购人或者其他供应商的合法权益情形的； | 否 |
| 9 | 附加条件 | 响应文件未含有采购人不能接受的附加条件的； | 否 |
| 10 | 其他无效情形 | 供应商、响应文件不存在不符合法律、法规和磋商文件规定的其他无效情形。 | 否 |

2 磋商、响应文件有关事项的澄清、说明或者更正和最后报价

2.1 磋商小组所有成员将集中与单一供应商分别进行磋商，并给予所有参加磋商的供应商平等的磋商机会。

2.2 在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

2.3 对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。

2.4 供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人（若供应商为事业单位或其他组织或分支机构，可为单位负责人）或授权代表签字或者加盖公章。由授权代表签字的，应当附授权委托书。供应商为自然人的，应当由本人签字并附身份证明。

2.5 响应文件的澄清、说明或者更正：

2.5.1 磋商小组在对响应文件的有效性、完整性和响应程度进行审查时，可以要求供应商对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容等作出必要的澄清、说明或者更正。

2.5.2 磋商小组对响应文件进行审查，如发现供应商提交的响应文件存在不满足《符合性审查要求》的内容，如属于表中“不允许”澄清、说明或者更正的内容，则供应商响应文件按**无效处理**；如属于表中的“允许”澄清、说明或更正的内容，磋商小组将要求供应商在规定的时间内对响应文件进行澄清、说明或者更正。如供应商在磋商小组规定的时间内未作出必要的澄清、说明或者更正，或澄清、说明或者更正后仍不

能满足采购文件要求的，则供应商的响应文件按**无效处理**。

2.5.3 供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。磋商小组要求供应商澄清、说明或者更正响应文件应当以书面形式作出。供应商的澄清、说明或者更正应当由法定代表人（若供应商为事业单位或其他组织或分支机构，可为单位负责人）或其授权代表签字或者加盖公章。由授权代表签字的，应当附授权委托书。供应商为自然人的，应当由本人签字并附身份证明。澄清、说明或者更正文件将作为响应文件内容的一部分。

2.6 磋商结束后，磋商小组将要求所有实质性响应的供应商在规定时间内提交最后报价。最后报价时间为磋商小组指定的时间，具体时间根据磋商进度另行通知。

2.7 异常低价处理

2.7.1 政府采购评审中出现下列情形之一的，评审委员会应当启动异常低价投标（响应）审查程序：

（1）投标（响应）报价低于全部通过符合性审查供应商投标（响应）报价平均值 50%的，即投标（响应）报价<全部通过符合性审查供应商投标（响应）报价平均值×50%；

（2）投标（响应）报价低于通过符合性审查的次低报价供应商投标（响应）报价 50%的，即投标（响应）报价<通过符合性审查的次低报价供应商投标（响应）报价×50%；

（3）投标（响应）报价低于采购项目最高限价 45%的，即投标（响应）报价<采购项目最高限价×45%；未设定最高限价的采购项目，以采购项目预算金额作为最高限价；

（4）评审委员会基于专业判断，认为供应商报价过低，有可能影响产品质量或者不能诚信履约的其他情形。

2.7.2 评审委员会启动异常低价投标（响应）审查后，属于前述第（1）项至第（4）项情形的，应当要求相关供应商在评审现场合理的时间内对投标（响应）价格作出解释，提供项目具体成本测算等与报价合理性相关的书面说明及必要的证明材料，包括但不限于原材料成本、人工成本、制造费用等，给予相关供应商的合理时间一般不少于 30 分

钟。其中，属于第（3）项情形，供应商已随投标（响应）文件一并提交相关书面说明及必要的证明材料的，在评审现场可不再重复提交。

2.7.3 评审委员会依据专业经验，参考同类项目中标（成交）价格、类似产品市场价格水平、行业人工费用标准、国家有关部门指导行业协会发布的行业平均成本等情况，对报价合理性进行判断。投标（响应）供应商不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，评审委员会应当将其作为无效投标（响应）处理。

2.7.4 上述投标（响应）报价指按照本章 3.2 修正后的报价。

2.8 磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组应当要求所有实质性响应的供应商在规定时间内提交最后报价，提交最后报价的供应商不得少于 3 家。磋商文件不能详细列明采购标的的技术、服务要求，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价。市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目，提交最后报价的供应商可以为 2 家；政府购买服务项目（含政府和社会资本合作项目），在采购过程中符合要求的供应商（社会资本）只有 2 家的，竞争性磋商采购活动可以继续进行。

2.9 最后报价是供应商响应文件的有效组成部分。

2.10 已提交响应文件的供应商，在提交最后报价之前，可以根据磋商情况退出磋商。

3 最后报价的算术修正及政策调整

3.1 最后报价须包含竞争性磋商文件全部内容，如最后分项报价表有缺漏视为已含在其他各项报价中，将不对最后报价进行调整。磋商小组有权要求供应商在评审现场合理的时间内对此进行书面确认，供应商不确认的，视为将一个采购包中的内容拆分响应，其**响应无效**。

3.2 最后报价出现前后不一致的，按照下列规定修正：

3.2.1 竞争性磋商文件对于报价修正是否另有规定：

□有，具体规定为：_____

■无，按下述 3.2.2-3.2.5 项规定修正。

3.2.2 大写金额和小写金额不一致的，以大写金额为准；

3.2.3 单价金额小数点或者百分比有明显错位的，以总价为准，并修改单价；

3.2.4 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

3.2.5 同时出现两种以上不一致的，按照前款规定的顺序修正。

3.2.6 修正后的报价经供应商书面确认后产生约束力，供应商不确认的，**其响应无效**。

3.3 落实政府采购政策的价格调整：只有符合第二章《供应商须知》4.3 条规定情形的，可以享受中小企业扶持政策，用扣除后的价格参加评审；否则，评审时价格不予扣除。

3.3.1 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对小微企业报价给予 10 %的扣除，用扣除后的价格参加评审。

3.3.2 对于未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，且接受大中型企业与小微企业组成联合体或者允许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的联合体或者大中型企业的报价给予 / %的扣除，用扣除后的价格参加评审。

3.3.3 组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

3.3.4 价格扣除比例对小型企业和微型企业同等对待，不作区分。

3.3.5 中小企业参加政府采购活动，应当按照竞争性磋商文件给定的格式出具《中小企业声明函》，否则不得享受相关中小企业扶持政策。

3.3.6 监狱企业提供了由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件的，视同小微企业。

3.3.7 残疾人福利性单位按竞争性磋商文件要求提供了《残疾人福利性单位声明函》的，视同小微企业。

3.3.8 若供应商同时属于小型或微型企业、监狱企业、残疾人福利性单位中的两种及以上，将不重复享受小微企业价格扣减的优惠政策。

3.4 支持本国产品政府采购的价格调整：只有符合第二章《供应商须知》4.2 条规

定情形的，可以享受本国产品支持政策，用扣除后的价格参加评审；否则，评审时价格不予扣除。

3.4.1 本项目既有本国产品又有非本国产品参与竞争的，依法对本国产品给予价格评审优惠，对本国产品的报价给予 20%的价格扣除，用扣除后的价格参与评审。

3.4.2 当采购项目或者采购包中含有多种产品，供应商为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到 80%以上时，依法对该供应商提供的全部产品给予价格评审优惠，即对该供应商提供的全部产品的总报价给予 20%的价格扣除，用扣除后的价格参与评审。

3.4.3 供应商提供本国产品参加政府采购活动的，应当按照采购文件给定的格式出具《关于符合本国产品标准的声明函》或提供财政部会同有关部门规定的有关证明文件，否则视为非本国产品。

4 磋商环节及提交最后报价后如出现以下情况的，供应商的**响应文件无效**：

4.1 供应商对实质性变动不予确认的；

4.2 不满足磋商文件★号条款或磋商文件技术指标超出磋商文件《采购需求》中主要技术参数允许偏差的最大范围的（如有）；

4.3 未按照磋商小组规定的时间、逾期提交最后报价的；

4.4 如供应商的最后报价超过竞争性磋商文件中规定的项目/采购包预算金额或者项目/采购包最高限价的；

4.5 响应文件中出现可选择性或可调整的报价的（竞争性磋商文件另有规定的除外）；

4.6 最后报价出现前后不一致，供应商对修正后的报价不予确认的；

4.7 其他：/。

5 评审方法和评审标准

5.1 本项目采用的评审方法为：本项目的评审采用综合评分法。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

5.2 竞争性磋商文件中没有规定的评审标准不得作为评审依据。

5.3 非政府强制采购的节能产品或环境标志产品，依据品目清单和认证证书实施

政府优先采购。优先采购的具体规定（如涉及）__/__。

6 确定成交候选人名单

6.1 磋商小组将根据各供应商的评审排序以及磋商文件中关于成交候选人的相关规定，确定本项目成交候选人名单，按照评审得分由高到低顺序推荐成交候选人的排名顺序。评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。响应文件满足竞争性磋商文件全部实质性要求，且按照评审因素的量化指标评审得分最高的供应商为排名第一的成交候选人。评分分值计算保留小数点后两位，第三位四舍五入。

6.2 磋商小组根据上述供应商排序，依次推荐排序前__3__名的供应商为成交候选供应商（若在磋商文件允许的情形下提交最后报价的供应商为二家，则依次推荐二名供应商为成交候选供应商），并编写评审报告。

6.3 磋商小组要对评分汇总情况进行复核，特别是对排名第一的、报价最低的、响应文件被认定为无效的情形进行重点复核。

7 报告违法行为

7.1 磋商小组在评审过程中发现供应商有行贿、提供虚假材料或者串通等违法行为时，应当及时向财政部门报告。

## 二、评审标准

| 序号 | 评审因素 | 评标标准 | 分值 |
|---|---|---|---|
| 一、价格部分（10 分） | | | |
| 1 | 价格 | 满足磋商文件要求的最后报价最低的供应商的价格为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：磋商报价得分=（磋商基准价/最后报价）×分值。<br>此处最后报价指经过报价修正，及因落实政府采购政策进行价格调整后的报价，详见第三章《评审方法和评审标准》3.2、3.3及3.4。 | 10 |
| 二、商务部分（2 分） | | | |
| 2 | 类似业绩 | 供应商自2023年1月至今（以合同签订时间为准）承担过的与本项目类似的项目业绩，每有一个有效业绩得1分，本项最高得2分。<br>注：供应商应提供合同关键页复印件（至少包含合同首页、合同主要内容页、合同盖章页）并加盖供应商公章作为证明材料。否则该业绩不予认可。 | 2 |
| 三、技术部分（88 分） | | | |
| 3 | 流量服务方案 | **供应商须针对第四章采购需求中“2.1.2 移动警务流量110GB需求”的“单警应用支撑服务需求”全部内容进行承诺，承诺完全满足全部上述需求内容，须提供承诺函并加盖供应商单位公章，否则本项“流量服务方案”不得分。**<br>在此基础上：<br>**供应商应针对第四章采购需求中“二、采购需求”中的“2.1流量服务需求”提供服务方案：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得7分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得5分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得3分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得1分；<br>未提供相关内容不得分。 | 7 |
| 4 | 链路服务方案 | **供应商应针对第四章采购需求中“二、采购需求”中的“2.2链路服务需求”提供服务方案：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得7分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实 | 7 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| | | 际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 3 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。 | |
| 5 | 移动警务增值服务方案 | **供应商应针对第四章采购需求中“二 采购需求”中“2.3 移动警务增值服务需求”中的“2.3.1 移动互联网基础服务需求”、“2.3.2 联网服务区基础设施服务需求”、“2.3.3 移动安全接入基础服务需求”、“2.3.4 公安信息网安全服务需求”、“2.3.5 移动互联网区应用支撑使用服务需求”、“2.3.6 联网服务区应用支撑使用服务需求”、“2.3.7 业务应用使用服务需求”、“2.3.8 移动警务安全管控服务需求”、“2.3.9 移动警务基础安全设施服务需求”、“2.3.10 合规性检测服务需求”共计 10 项内容提供服务方案：**<br>每具有 1 项方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>每具有 1 项方案方案内容全面、能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>每具有 1 项方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>每具有 1 项方案的响应仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>每具有 1 项方案未提供的，该项方案不得分。<br>本部分共计 10 项，每项满分 2 分，本部分最高得 20 分。 | 20 |
| 6 | 服务承诺 | 供应商提供承诺函，承诺基础设施安全服务所涉及的设备具有原厂授权及原厂售后服务的，得 2 分，否则不得分。<br>提供承诺函（格式自拟）并加盖供应商公章。 | 2 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| 7 | 其他服务 | **供应商针对第四章采购需求“三 其他服务”中“3.1 移动警务整体支撑服务要求”中的“3.1.1 日常支撑服务要求”、“3.1.2 重大重要节庆假日期间的支撑服务要求”“3.1.3 终端使用支撑服务要求”“3.1.4 运营开发服务要求”提供服务方案：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 4 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 3 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 2 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。 | 4 |
| 8 | 移动警务租用服务时限承诺 | **供应商针对第四章采购需求“三 其他服务”中“3.2 移动警务租用服务时限要求”提供承诺函：**<br>提供了承诺函且承诺完全满足本项目“三 其他服务”中“3.2 移动警务租用服务时限要求”的全部内容得 2 分，否则不得分。<br>提供承诺函（格式自拟）并加盖供应商公章。 | 2 |
| 9 | 团队人员承诺 | **供应商针对第四章采购需求“三 其他服务”中“3.3 团队人员”提供承诺函：**<br>提供了承诺函且承诺拟派本项目的团队人员完全满足本项目“3.3 团队人员”的全部内容得 2 分，否则不得分。<br>提供承诺函（格式自拟）并加盖供应商公章。 | 2 |
| 10 | 整体服务设计方案（一） | **供应商针对第四章采购需求“四、整体服务设计要求”中 4.1 项要求提供北京市公安局移动警务泛物联终端接入和管理设计方案：**<br>**（1）提供泛物联终端直连、桥接型接入认证、访问控制和数据服务标准化的技术实现方案，要求方案包含数据流转图，且符合公安行业规范与移动警务业务需求：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 2 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。 | 10 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| | | **（2）提供云端与边缘端对泛物联终端的管控技术实现方案，要求方案包含业务架构图，合理覆盖各类终端（移动警务终端、智能传感设备、移动执法终端等）管控项及技术手段：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 2 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。<br>**（3）提供泛终端智能协同整体技术架构和方案，要求方案包含云边端服务设计、数据流转图，且完全符合公安行业规范与移动警务安全入网需求：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 2 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。<br>**（4）提供泛物联终端接入管理功能模块详细介绍：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 2 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。 | |
| 11 | 整体服务设计方案（二） | **供应商针对第四章采购需求“四、整体服务设计要求”中 4.2 项要求提供北京市公安局移动警务音视频平台整体设计方案：**<br>**（1）提供移动警务音视频采集、传输、存储、分发全流程技术** | 6 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| | | **方案，要求方案包含业务架构图，覆盖图传互动、视频调阅、远程会商等场景，符合公安音视频技术规范：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（2）提供音视频平台与现有公安视频系统、指挥调度系统对接方案，要求方案包含逻辑架构图，明确对接标准、数据格式及安全管控措施：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（3）提供音视频平台核心功能模块详细说明：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。 | |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| 12 | 整体服务设计方案（三） | **供应商针对第四章采购需求“四、整体服务设计要求”中 4.3 项要求提供北京市公安局 AI 助手技术方案和标准化接入方案：**<br>**（1）提供移动警务 AI 助手核心技术方案，包含且不仅限于含语音交互、智能检索、业务辅助、安全防护等，要求方案包含业务架构图，符合公安数据安全规范与移动警务轻量化应用需求：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（2）提供 AI 助手标准化接入技术方案，要求方案包含数据流转图，明确接入协议、接口规范、适配标准，支持与移动警务平台、公安业务系统无缝对接：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（3）提供 AI 助手技术模块功能详细说明：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解 | 6 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| | | 错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。 | |
| 13 | 整体服务设计方案（四） | **供应商针对第四章采购需求“四、整体服务设计要求”中 4.4 项要求提供北京市公安局移动端门户设计方案（包括认证、应用形态、流程等）：**<br>**（1）提供移动端统一门户整体架构设计方案，要求方案包含业务架构图，整合移动警务各类应用形态技术方案，符合公安移动应用建设规范：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。<br>**（2）提供新门户统一身份认证方案（含多因子认证、权限分级、安全审计），要求方案包含逻辑架构图，认证流程、权限控制逻辑，符合公安身份安全管理规范，保障门户访问安全：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 2 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。<br>**（3）提供门户应用形态设计（含元服务、卡片、多媒体消息等）与门户自定义的技术方案，要求方案包含业务示例、数据流转、自定义技术方案、与第三方移动警务平台和应用的对接关系等逻辑：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 2 分； | 10 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| | | 方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。<br>**（4）提供移动端统一门户核心功能详细说明**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2.5 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 2 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1.5 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 1 分；<br>未提供相关内容不得分。 | |
| 14 | 整体服务设计方案（五） | **供应商针对第四章采购需求“四、整体服务设计要求”中 4.5 项要求提供北京市公安局移动警务业务应用迁移过程保障业务连续性的支撑设计方案：**<br>**（1）提供移动警务业务应用现状分析方案，要求方案包含逻辑架构图、现状痛点及迁移需求分析，贴合移动警务实际业务运行情况：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（2）提供应用迁移网络部署与安全隔离方案，要求方案包含网络部署图，符合公安移动警务网络安全规范，保障迁移过程数据安全与网络稳定：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的， | 6 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| | | 得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（3）提供迁移过程业务连续性保障方案，要求包含风险评估、分阶段迁移计划、资源配置、应急处置与回退机制，确保迁移期间业务无中断、数据无丢失：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。 | |
| 15 | 整体服务设计方案（六） | **供应商针对第四章采购需求“四、整体服务设计要求”中 4.6 项要求提供北京市公安局泛终端接入开发者管理和技术支撑方案：**<br>**（1）提供泛终端接入开发者全生命周期管理方案，要求包含清晰的管理流程图（涵盖开发者注册、产品注册、认证、产品上架、审批等环节）：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（2）提供与泛终端智能协同云服务管理平台的技术对接方案，明确对接关系，对接形式（如 REST API、消息队列、数据同步）、数据依赖关系：** | 6 |

| 序号 | 评审因素 | 评标标准 | 分值 |
| --- | --- | --- | --- |
| | | 方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。<br>**（3）提供终端开发者管理核心功能详细说明：**<br>方案内容全面完善并根据本项目需求进行了详细论述，方案贴合本项目实际需求且包含具体的实施细节及有效措施，完全满足采购需求的，得 2 分；<br>方案内容全面、方案能满足采购需求，方案内容贴合本项目实际需求并包含具体的实施细节及有效措施，但阐述不详细的，得 1.5 分；<br>方案内容全面、能满足采购需求，但方案中未包括具体实施细节及措施或未贴合项目实际情况进行详细论述的，得 1 分；<br>提供了方案，但方案仅为对采购需求的简单复制，或存在理解错误、或内容与事实不符、或不符合采购需求情况的，得 0.5 分；<br>未提供相关内容不得分。 | |
| 合计 | | | 100 |

# 第四章　采购需求

## 一 项目概况

北京市公安局拟为每名民警配备移动警务终端，采用运营商合约流量套餐方式购置。通过竞争性磋商方式确定 1 家成交供应商，市局直属单位及各分局自行分批次与成交供应商签订合同，服务周期为 3 年。

## 二 采购需求

### 2.1 流量服务需求

#### 2.1.1 群发短信服务需求

根据移动警务业务需求，提供支持三网统一的短信发送服务，服务要求为 200 万条/年。

#### 2.1.2 移动警务流量 110GB 需求

**1. 110G（专网+互联网）**

流量共享池要求：流量套餐的流量，应建立以市局及各分局的流量共享池，具备流量提示及限制功能，当月没使用流量自动转入下月流量中，供应商需对超流量池部分流量费单价进行说明。

测试卡要求：要求提供不少于 65 张测试 SIM 卡，按照套餐提供并可接入移动警务平台。

其他要求：要求提供的 SIM 卡号段为连续整号段。

**2. 单警应用支撑服务需求**

单警应用支撑服务包含移动警务终端及其配件服务，移动警务终端应选用国产品牌，要求终端版本提供定期升级服务，升级次数不低于 1 次/年。

**（1）北京市公安局单警应用支撑服务的警务终端及其配件要求**

移动警务终端需按照 100%配置终端保护壳，并每年为市局提供 40 台指定终端作为测试机。

提供不低于流量套餐总量 5‰的备用服务，包含移动警务终端及配件。如果所投服务的终端产品停产或无法供货的情况下，要升级到同品牌系列的下一代产品。

- **移动警务终端要求**

符合 GA/T 1466.1-2018 《智能手机型移动警务终端 第 1 部分：技术要求》中多模

终端（个人普通终端+增强受控终端）要求，并取得相关资质认证。可根据不同的使用环境切换不同的操作系统。安全模式下操作系统接受专用管理进行统一认证和设备绑定，进入安全区受到保护。

具备电信设备进网许可证、无线电发射设备型号核准证、中国国家强制性产品（3C）认证。

服务要求：

根据公安部的入围标准，考虑实际的使用需求，项目的终端选型标准参数如下：

处理器：不低于 8 核高性能芯片，最高主频不小于 2.4GHz。

屏幕不低于 6.7 英寸，OLED 屏。

分辨率不低于 2800×1250。

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。

前置摄像头：不低于 1 个 1200 万像素超广角摄像头和 1 个 3D 深感摄像头。

运行内存：不小于 12G。机身内存：不小于 256G。

电池容量：不低于 5700mA（额定值），支持不低于 66W 有线超级快充，支持不低于 50W 无线超级快充，支持反向充电。

NFC：内置 NFC 模块，支持读卡器模式，卡模拟模式。

防护能力：支持在 GB/T 4208-2017（国内）标准下达到 IP68 级防尘抗水能力。

蓝牙：5.2 及以上，支持低功耗蓝牙。

传感器：支持重力传感器、红外传感器、霍尔传感器、陀螺仪、指南针、环境光传感器、接近光传感器、Camera 激光对焦传感器、色温传感器。

卫星通信：为保障应急和极端场景下的通信要求，所投移动警务终端可在无地面网络信号覆盖或网络中断的环境下，支持文字卫星消息收发功能。

定位：支持北斗独立定位功能，仅用北斗卫星信号进行搜星、捕获、定位解算和输出。

操作系统：支持基于国产自主操作系统开发的安全双系统，可按需适配生态应用和系统版本定制。

双系统隔离：两个操作系统运行在不同 ROM 空间，独立运行，完全隔离；两个系统的文件系统、网络连接、外围接口、用户数据都彼此隔离，不能相互访问；任何一个系统不能删除、创建或控制另外一个系统；一个系统重置不影响另外有一个系统。

双系统同时在线：支持公共 APN 和专属 APN 同时接入、同时在线。当前系统能接收到另外一个系统的通知栏消息，但看不到数据。

按要求定制开机画面及 LOGO。

具备空中发证所必需的安全模块的警务通加解密服务，并实现证书远程管理功能，具有商用密码产品认证证书。

具有服务厂家针对本项目终端安全芯片发证认证服务有效的授权书。

需求数量：54672 台。

- **终端保护壳要求**

满足 1.2 米跌落防摔情况下，终端应无明显损伤且不影响正常使用；采用黑色+深蓝外观，具备变向支架功能，具有统一的北京公安标识。

需求数量：54672 个。

- **专业充电背夹要求**

双操作系统普通安全单警应用支撑持续供电服务。

电池容量不低于 10000 毫安，与单警应用支撑保护服务的警务终端紧密贴合；

满足 1.2 米跌落防摔；具有统一的北京公安标识。

需求数量：27336 个。

- **其他配件要求**

提供可将终端固定于执法车警用执法汽车支架，便于民警日常使用和抓拍违法，数量不低于 1000 套。

- **移动警务办公终端要求**

基础资质：所投产品具备电信设备进网许可证、无线电发射设备型号核准证、中国国家强制性产品（3C）认证证书、中国节能认证产品认证证书。

硬件要求：

处理器：不低于 8 核高性能芯片，最高主频不小于 2.4GHz。

屏幕：不低于 11.5 英寸，分辨率不低于 2200×1440，10 点触控，支持触控笔功能。

摄像头：支持拍照、录像功能，主摄不低于 1300 万像素，前摄不低于 800 万像素。

运行内存：不低于 8G。

机身内存：不低于 128G，并能支持 microSD 存储卡。

电池：电池容量不低于 7700mA。

蓝牙：蓝牙 5.2，支持 BLE,支持 SBC、AAC,支持 LDAC 高清音频。

WiFi：IEEE 802.11 a/b/g/n/ac/ax，2.4G/5G，加密方式：支持 WPA/WPA2/WPA3。

传感器：支持重力传感器、环境光传感器、指南针。

定制要求：

增强型受控终端：满足移动警务增强型受控终端技术要求并获得检测报告。

系统安全：系统需防 Root，禁止刷机成普通消费者版本。

安全水印：支持系统级全局水印功能，防止偷拍屏幕造成信息泄露，同时支持防截屏、防录屏。

配件需求：配备触控笔、支架保护壳、贴膜等。

需求数量：145 个。

**（2）终端预置服务要求**

- **终端系统开放原生服务要求**

在单警应用支撑终端系统上开放系统原生的服务，面向上层应用提供终端侧服务能力，终端原生服务能力包括：离线人脸识别、卡证识别、车牌识别，要求此类服务支持私有化或者支持无需联网终端本地化服务。

在单警应用支撑终端上提供原生系统终端助手的能力，系统终端助手支持热键唤起，同时，支持对终端的主要功能的控制，包括且不仅限于：摄像头、麦克风、打开应用等终端侧服务，同时，该原生系统终端助手还需支持集成第三方业务平台开放的能力，基于用户的输入准确识别用户诉求，并调用对应的服务能力实现业务闭环。

系统开放多媒体消息提醒服务，支持系统推送、实况窗、VoIP 消息等，支持在符合技术规范的要求下实现个人域和安全域的消息同步、通讯录同步、照片同步和视频同步。

- **终端预置自定义门户服务要求**

在单警应用支撑终端、移动警务办公终端负一屏集成自定义门户，支持集成卡片、元服务、原生应用的统一入口，实现终端系统账号与统一认证的打通。

终端人脸识别登陆系统模式与统一认证服务打通，实现强绑定认证。区分终端登陆模式与其他认证方式进入终端后的权限级别，人脸识别通过认证后系统进入已认证状态；其他登陆方式使用移动应用需要进行二次认证。

要求所提供的移动终端上预置自定义门户，门户中可灵活配置基础服务组件。要求在终端开通后默认可使用以下服务内容，包括但不限于：

整合消息中心、预警中心、任务中心服务能力。

整合元服务能力，包括：签到、热线等。

整合卡片服务能力，包括：人工智能助手入口、图传、视频会议、打卡、日历、警务新闻、规范条例等。

整合系统功能，包括：扫一扫、首都公安、首都警务报道、云盘等。

支持不少于 6 万终端的使用需求，要求门户打开时间不高于 3 秒。

- **终端预置 VPN 证书客户端服务要求**

根据平台提供的 VPN 服务，终端出厂时需预置相应的 VPN 终端客户端，并对应用进行保活，避免进程被误杀。

对接 VPN 的标准接口，实现对 VPN 的启动、监控、连接保活等能力。

- **终端预置泛终端智能协同服务客户端版本服务要求**

要求所提供的移动终端上预置泛终端智能协同服务客户端服务框架及其内部组件，并要求对该服务框架和内部组件进行保活，提供泛终端消息提醒服务、统一的认证和账户服务、扩展终端接入认证服务等终端侧服务能力。泛终端智能协同服务客户端服务框架主要实现对内部组件的统一管理和调用，内部组件统一按照泛终端智能协同服务框架的标准要求视线对接，当前包含的组件有：

泛终端消息提醒组件：包含语音、震动、弹窗、推送、喇叭音等消息提醒的组件。

移动终端安全管理服务组件：实现对终端的安全管控。

提供移动警务应用监管服务：提供对应用的使用监管服务。

终端预置证书管理客户端服务：国密 PKI 体系的证书管理客户端服务。

网络服务组件：实现基于业务的终端组网服务，支持 WLAN 和蓝牙。

账户服务组件：支持对上层或者终端的统一账号管理和认证转发服务，协同基础库和证书，实现应用、设备的认证。

授权组件：支持对终端侧网络接入、连接、组网和服务调用的授权转发。

## 2.2 链路服务需求

根据全国公安移动警务升级改造建设任务书要求，以及移动警务的业务情况，对移动警务专线接入提出如下需求。

### 2.2.1 专线接入服务需求

1. 提供到市局的 APN/VPDN 专线 10G，数量 1 条，要求主备链路。

2. 提供到市局的物联网专线 30G，数量 1 条，要求主备链路。

3. 提供移动互联网专用接入链路，带宽不低于 1G，数量 1 条，主备实现链路冗余，公网 IP 数量不少于 255 个。

4. 提供从公有云到移动互联网服务子平台的点对点专用链路，带宽不低于 1G，数量 1 条。

5. 提供市局到分局的点对点专线（接入网络-星型网络）10G，数量 17 条。

6. 提供市局到分局的点对点专线（互联网络-星型网络）10G，数量 17 条。

7. 提供分局之间的点对点专线（互联网络-环型网络）10G，双物理链路，数量 17 条。

8. 提供派出所、交通支大队二类区接入千兆专线，数量 512 条。

9. 提供直属单位二类区接入的千兆专线，数量 28 条。

10. 提供应急备用专线千兆专线，数量 10 条。

移动警务服务提供 APN/VPDN 专用通信网络专线的认证模式为自建 AAA 模式，由采购人管控。

移动警务服务提供 APN/VPDN 专用通信网络，需保证移动警务终端经无线传输链路到公安侧接入专线的信息通信安全。禁止非公安授权用户通过配置 APN 账号信息接入公安 APN/VPDN 专用通信网络。

移动警务服务业务中使用的 APN/VPDN 域名、移动警务专用 SIM/UIM 卡数据支持全国漫游服务。

移动警务服务业务的整个通信链路不被旁路，移动警务专用 SIM/UIM 卡不能接入互联网（用于多模式/系统移动警务终端的专用 SIM/UIM 卡另行要求），无线传输链路及 VPN 专线需与互联网通道进行有效隔离。

移动警务服务提供的 APN/VPDN 专用通信网络，从移动警务终端到公安侧接入专线之间，为采购人分配除 10.0.0.0/8、14.0.0.0/8、15.0.0.0/8、16.0.0.0/8（公安信息网）、20.0.0.0/8（公安移动信息网）等以外的 IP 地址网段。

除了满足以上对带宽要求外，还需要根据市局的业务情况动态调整带宽，实际负载峰值不能超过链路带宽 60%。

通信网络性能质量满足以下要求：

1. 吞吐量（Throughput）：签约带宽的 100%（合格值）。

2. 丢包率（Frame Loss）：≤0.1%（合格值）。

3. 时延：本地小于 20ms。

4. 接口误码性能要求：在规定条件范围内工作时，自环连续测试 24 小时应无误码。

5. 接入链路的端到端全程监控管理，充分保障用户电路的安全可靠性，及电路开

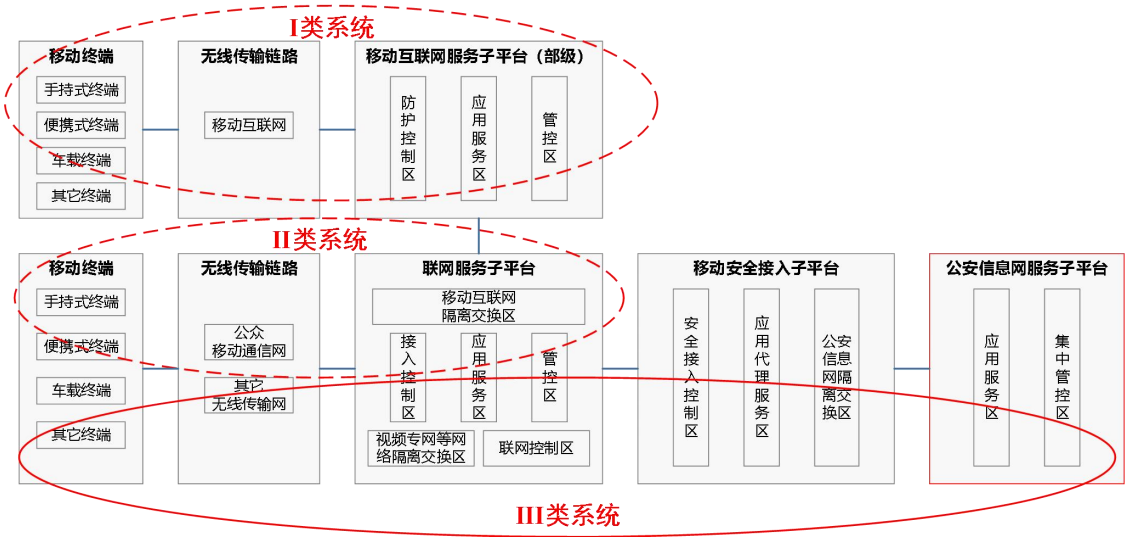
通和调配的及时性和灵活性。

6. 电路具有自愈保护功能，在光纤损坏、光接口损坏情况下，租用的电路可用率达到 99.9%。

7. 供应商应确保采购人在北京市行政区域内的有效通信，在发现信号盲区时能及时补盲。

## 2.3 移动警务增值服务需求

移动警务基础设施服务应根据公安部建设任务书规划以及相关移动警务系统建设规范的要求，满足等保 2.0 二级标准,满足 11 万终端用户的接入，包含移动互联网基础服务、联网服务区基础设施服务、移动安全接入基础服务和公安信息网基础服务四部分，整体架构如下：




### 2.3.1 移动互联网基础服务需求

#### 2.3.1.1 云资源使用服务需求

提供弹性可扩展的计算服务能力，配置要求是 1000 个虚拟核 CPU、2T 内存，1.5P 的块存储，资源可以进行自主配置，要求提供服务器应用负载能力，符合等保 2.0 二级对云安全的要求；要求公有云的业务网络与互联网逻辑隔离，并且提供公有云到移动互联网服务子平台的点对点专用冗余链路。云资源要求满足公安网软硬件负载需求支持后续随应用扩展，增加相应硬件资源。

#### 2.3.1.2 网络服务需求

**1. 链路接入交换服务**

交换容量不低于 180Gbps；包转发率不低于 50Mpps；千兆电口不低于 20 个，千兆光口不低于 4 个，要求满配光模块，能够实现设备堆叠、设备冗余。

**2. 核心交换服务**

包转发不低于 24000 Mpps，单台设备的主控、电源要求冗余，万兆光口数量不低于 30 个，万兆多模光模块满配，千兆光口数量不低于 48 个，千兆多模光模块满配，千兆电口不低于 48 个，能够实现设备堆叠、设备冗余。

**3. 接入交换服务**

交换容量不低于 550Gbps；包转发率不低于 180Mpps；千兆电口不低于 48 个，万兆光口不低于 4 个，要求满配多模光模块，能够实现设备堆叠、设备冗余。

### 2.3.2 联网服务区基础服务需求

联网基础服务主要提供网络基础服务和私有云服务。

物联网和移动警务专线接入链路通过市局统一路由接入，再通过点对点专线接入到各分局含交管总队。

分局含交管总队与市局之间要求采用星型网络加环状网络架构的形式，分局与分局通过环网互联，分局与市局通过星型网络互联。

#### 2.3.2.1 市局云资源使用服务需求

根据市局实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

**1. 弹性云服务节点 1 的要求**

要求提供 CPU、内存、镜像、云硬盘可随时获取、可扩展的弹性云服务计算节点；

服务器资源要求：所有服务器可提供的物理核总数不低于 4644 核，可提供的内存总数要求不低于 33024GB。

其中单台服务器配置要求如下：

CPU：配置不低于 2 颗处理器，单颗不低于 18 个物理核，主频不低于 2.2G HZ

内存：配置不低于 256G DDR4 内存，单根内存不低于 32G，主频不低于 2933 MHz

系统盘：配置不低于 2×600G 10K SAS 硬盘

Raid 卡：支持 RAID 0,1,10

网卡：配置 4×GE 电口，6×10GE 光口（要求满配多模光模块）

**2. 弹性云服务节点 2 的要求**

要求提供 CPU、内存、镜像、云硬盘可随时获取、可扩展的弹性云服务计算节点；

服务器资源要求：所有服务器可提供的物理核总数不低于 4032 核，可提供的内存总数要求不低于 24192GB，可用存储容量要求不低于 1.4PB（2 副本）。

其中单台服务器配置要求如下：

CPU：配置不低于 2 颗处理器，单颗不低于 32 个物理核，主频不低于 2.6G HZ，动态加速频率不低 3.4GHZ，L3 缓存不低于 36M。

内存：配置不低于 384G DDR4 内存，单根内存不低于 32G，主频不低于 3200 MHz

系统盘：配置不低于 2×480G 2.5 SATA 6Gb R SSD。

Raid 卡：支持 RAID 0,1,10。

网卡：配置 2×GE 电口，4×10GE 光口（要求满配多模光模块）。

可用存储容量要求，不低于 1.4PB（2 副本）：单节点配置不低于 12×3.84TB SSD SAS 盘。

**3. 弹性云服务节点 3 的要求**

要求提供 CPU、内存、镜像、云硬盘可随时获取、可扩展的弹性云服务计算节点；

服务器资源要求：所有服务器可提供的物理核总数不低于 7808 核，可提供的内存总数要求不低于 62464GB。

其中单台服务器配置要求如下：

CPU：配置不低于 2 颗处理器，单颗不低于 64 个物理核，主频不低于 2.6G HZ。

内存：配置不低于 1024G DDR4 内存，单根内存不低于 64G，主频不低于 4800MHz。

系统盘：配置不低于 2×480G SATA SSD 硬盘。

缓存盘：配置不低于 2×固态硬盘 3.84T SATA SSD（混合型）。

数据盘：配置不低于 8×10T 机械硬盘。

网卡：配置 4×GE 电口，2×10GE 光口，2×25GE 光口（要求满配多模光模块）。

**4. 编解码计算模块 1 的服务要求**

编解码计算模块：要求 GPU 加速型云服务器能够提供强大的浮点计算能力，满足高实时、高并发的海量计算场景。

要求提供不少于 8 个计算节点。单个节点要求配置如下：支持 x86 或 arm 架构，配置不低于 4 颗处理器（单颗处理器不低于 48 个物理核，主频不低于 2.6GHZ），内存不低于 1024G DDR4，2×480G SATA SSD 硬盘，2×3840G NVMe SSD 硬盘；支持 RAID 0/1/5/6，不少于 4 个千兆网口，8 个 200GE 光口，2 个 25GEg 光口，满配光模块，配置不低于 8 块 GPU 卡（处理器间支持 fullmesh 全互联，互联带宽最大不低于 392GB/s。单颗处理器 FP16 算力≥280TFLOPS；单颗处理器 HBM 显存≥64G）。

**5. 编解码计算模块 2 的服务要求**

编解码计算模块：要求 GPU 加速型云服务器能够提供强大的浮点计算能力，满足高实时、高并发的海量计算场景。

要求提供不少于 8 个计算节点。每个节点双路服务器处理器：支持 x86 或 arm 架构，配置不低于 2 颗处理器（单颗处理器不低于 48 个物理核，主频不低于 2.6GHZ），内存：不低于 256GB；磁盘：2×480GB SATA SSD，2×960GB SATA SSD；RAID 卡：4G Raid0/1/5/6 卡（带超级电容）；NPU 卡：不低于 8 块高性能 NPU 卡；网卡：不少于 4 个千兆网口，不少于 2 个 25GE 光口,满配光模块；其他：AC/DC 冗余电源，含服务器导轨，远程管理模块。

**6. 编解码计算模块 3 的服务要求**

编解码计算模块：要求 GPU 加速型云服务器能够提供强大的浮点计算能力，满足高实时、高并发的海量计算场景。

要求提供不少于 17 个计算节点。每个节点双路服务器处理器：支持 x86 或 arm 架构，配置不低于 2 颗处理器（单颗处理器不低于 48 个物理核，主频不低于 2.6GHZ），内存：不低于 256GB；磁盘：2×480GB SATA SSD，2×960GB SATA SSD；RAID 卡：4G Raid0/1/5/6 卡（带超级电容）；NPU 卡：不低于 6 块高性能 NPU 卡（单卡显存 48G,FP16 算力 70TFLOPS）；网卡：不少于 4 个千兆网口，不少于 2 个 25GE 光口,满配光模块；其他：AC/DC 冗余电源，含服务器导轨，远程管理模块。

**7. 存储节点 1 要求**

可用存储容量要求，不低于 2PB（2 副本）。

单节点配置不低于 36×8TB 7.2K RPM SATA 硬盘，2×600G 10K SAS 盘，2×3.2TB SSD NVMe 盘，2×3.84T 2.5 SATA 6Gb R SSD，CPU 数量不低于 2 个，主频不低于 2.3GHz，内存不低于 256 GB。网络接口不低 2×GE 电口，4×10GE 光口（要求满配多模光模块）。

**8. 存储节点 2（SSD）要求**

可用存储容量要求，不低于 200TB（2 副本）。

单节点配置不低于 2×600G 10K SAS 盘，36×3.84TB SSD SAS 盘，CPU 数量不低于 2 个，主频不低于 2.3GHz，内存不低于 256GB。网络接口不低 2×GE 电口，4×10GE 光口（要求满配多模光模块）。

**9. 存储节点 3（SATA）要求**

有效存储容量要求，不低于 8PB（2 副本）。

单节点配置不低于 2×480G 2.5 SATA SSD，4×3.84T-U.2 NVME SSD(读密集型)，

36×16TB 机械硬盘，CPU 数量不低于 2 个，核数不低于 24，主频不低于 2.6GHz，内存不低于 512GB。网络接口不低 4×GE 电口，4×25GE 光口（要求满配多模光模块）。

**10. 云的其他要求**

动态资源扩展：实现对应用资源的自动弹性扩展和人工弹性扩展两种方式。

提供云内安全服务。

云资源按需提供给物联网区域和联网服务区域，并在区域之间的资源进行安全隔离。

云资源根业务和数据部署区域划分业务域和数据域，数据域的访问需进行统一授权。

根据云节点的情况配置对应的云管服务。提供云管理软件，可接入现有公安网云平台，做到资源可被监管；要求市局云平台统一对分局云平台进行管理。关系型数据库 MySQL 等主流关系型数据库的管理平台。支持关系型数据库的自动化部署、自动主从切换,提供数据库备份和恢复等能力;提供正版原厂操作系统包括且不限于 Windows、Linux 等，操作系统授权数量根据实际的业务需求数提供；支持软负载功能，可为虚拟计算节点提供负载分担能力。要求为私有云提供网管服务。要求为私有云提供对应的核心网络设备、接入网络设备、管理网络设备，整体要求冗余性、支持 vxlan，主干链路的带宽不低于 40Gbps。提供云中间件服务和云容器化统一管理和调度服务，其中，容器化需按照服务器集群的总核数提供。

### 2.3.2.2 分局云资源使用服务需求

根据分局实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

**1. 计算节点 1**

提供 16 个分局云服务，每个分局的服务器不少于 2 台，每台服务器的配置要求如下：

CPU：配置不低于 2 颗处理器，单颗不低于 16 个物理核，主频不低于 3.1G HZ

内存：配置不低于 128G DDR4 内存，单根内存不低于 32G，主频不低于 3200 MHz

系统盘：配置不低于 2×480G 2.5 SATA 6Gb RSSD

数据盘：配置不低于 3.84×4 2.5 SAS 12GB R SSD×4

GPU 卡：配置不低于高性能 16GB 卡

Raid 卡：支持 RAID 0,1,10

网卡：配置 2×GE 电口，4×10GE 光口（要求满配多模光模块）

**2. 计算节点 2**

提供 16 个分局云服务，每个分局的服务器不少于 3 台，每台服务器的配置要求如下：

CPU：配置不低于 2 颗处理器，单颗不低于 32 个物理核，主频不低于 2.5G HZ

内存：配置不低于 512 DDR4 内存，单根内存不低于 32G，主频不低于 4800 MHz

系统盘：配置不低于 2×480G SATA SSD

网卡：配置 4×GE 电口，4×10GE 光口（要求满配多模光模块）

**3. 块存储节点要求**

提供 16 个分局的存储服务，配置要求如下：

可用存储容量要求，每个分局不低于 75TB（2 副本）。

存储硬盘可安装于计算节点服务器也可提供独立存储节点。

单节点配置不低于 2×480G 2.5 SATA 6Gb R SSD，8×3.84TB SSD SAS 盘，CPU 数量不低于 2 个，核数不低于 10，主频不低于 2.4GHz，内存不低于 128GB。网络接口不低 2×GE 电口，4×10GE 光口（要求满配多模光模块）。

### 2.3.2.3 市局网络服务需求

根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

**1. 提供核心交换服务**

要求交换容量不低于 206Tbps，要求包转发不低于 38400Mpps，单台设备的主控、电源要求冗余，40G 光口不低于 24 个，40G 万兆多模光模块不低于 4 个，万兆光口数量不低于 68 个，万兆多模光模块满配，千兆光口数量不低于 48 个，千兆多模光模块满配，千兆电口不低于 48 个，要求设备冗余。

**2. 提供云核心交换服务 1**

要求交换容量不低于 28.8Tbps，要求包转发不低于 6000Mpps，单台设备的主控、电源要求冗余，40G 光口不低于 24 个，40G 万兆多模光模块满配，万兆光口数量不低于 24 个，万兆多模光模块满配，数量不低于 4 台。

**3. 提供云核心交换服务 2**

要求交换容量不低于 102.4Tbps，要求包转发不低于 57600Mpps，单台设备的主控、电源要求冗余，40G 光口数量不低于 36 个，40G 多模光模块满配，万兆光口数量不低于 48 个，万兆多模光模块满配，要求设备冗余。

**4. 接入管理交换服务**

要求交换容量不低于590Gbps；包转发率不低于190Mpps；千兆电口不低于48个，万兆光口不低于4个，配置不低于4个万兆多模光模块，能够实现设备堆叠，数量不低于56台。

**5. 提供业务接入交换服务**

要求交换容量不低于4.8Tbps；包转发率不低于2000Mpps；万兆光口不低于48个，满配万兆多模模块，40G光口不低于4个，满配40G多模光模块，能够实现设备堆叠，数量不低于34台。

**6. 提供存储接入交换服务**

要求交换容量不低于8Tbps；包转发率不低于3000Mpps；25G光口不低于48个，满配25G多模光模块，40G光口不低于8个，满配40G多模光模块。能够实现设备堆叠，设备数量不低于12台。

**7. 提供业务算力交换服务**

要求交换容量不低于51.2Tbps；包转发率不低于19200Mpps；提供不低于8个插卡槽位，不低于5个模块化风扇，不低于4个模块化电源；200G光口不低于24个，满配200G多模光模块，不低于2个万兆光接口；能够实现设备堆叠，设备数量不低于2台。

**2.3.2.4 分局网络服务需求**

根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

**1. 联网服务区分局网络服务**

分局、交管总队和其他分支点分别提供交换服务，要求单台交换容量不低于580Gbps；包转发率不低于180Mpps，提供不低于48口千兆电口，不低于8个万兆光口，要求电源冗余，要求配置万兆堆叠电缆，数量不低于34台。

分局、交管总队和其他分支点提供云交换服务，要求支持不低于48个万兆光口,4个40G光口，要求满配光模块，数量不低于34台。

**2. 派出所、交通大队网络服务**

派出所分支节点提供交换服务，要求单台交换容量不低于672Gbps,包转发率不低于126Mpps,提供不低于28个10/100/1000BASE-T端口,4个1G/10G BASE-X SFP Plus端口，支持1个管理用以太网口；数量不低于512台。

**3. 市局到直属单位网络服务**

交通支大队分支节点提供交换服务，要求单台交换容量不低于672Gbps,包转发率不

低于 126Mpps,提供不低于 28 个 10/100/1000BASE-T 端口,4 个 1G/10G BASE-X SFP Plus 端口，支持 1 个管理用以太网口；数量不低于 28 台。

**4. 提供应急备用专线网络服务**

提供应急备用交换服务，要求单台交换容量不低于 672Gbps,包转发率不低于 126Mpps,提供不低于 28 个 10/100/1000BASE-T 端口,4 个 1G/10G BASE-X SFP Plus 端口，支持 1 个管理用以太网口；数量不低于 10 台。

**5. 交管总队网络服务**

提供业务接入交换服务要求交换容量不低于 4.8Tbps；包转发率不低于 2000Mpps；万兆光口不低于 48 个，满配万兆多模模块；能够实现设备堆叠，数量不低于 2 台。

**6. 公交总队网络服务**

提供业务接入交换服务要求交换容量不低于 4.8Tbps；包转发率不低于 2000Mpps；万兆光口不低于 48 个，满配万兆多模模块；能够实现设备堆叠，数量不低于 2 台。

### 2.3.3 移动安全接入基础服务需求

#### 2.3.3.1 安全接入控制服务需求

安全接入控制服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

**1. VPN**

提供 VPN 接入服务，支持同时在线用户数不少于 11 万终端，要求支持安卓、鸿蒙、统信等操作系统。

**（1） VPN 集群 1:**

VPN 集群：网络带宽支持千兆，需采用标准 SSL、TLS 协议提供虚拟隧道网络服务，提供基于 TCP、UDP、ICMP 等 IP 层以上的协议的应用服务；提供的 VPN 服务需要支持现有移动警务认证方式，包括但不限于 INSE 模式下国密 SM2 证书结合认证、SIM 卡贴膜卡国密 SM2 证书结合认证、SIM 卡贴膜卡商密 RSA 证书结合认证，支持伪装服务器地址功能，VPN 服务可以将真实的服务器地址伪装成域名形式。实现认证、访问控制、加密传输，并发用户数≥1000,4M 码流；VPN 网关拨号时间<5S；接入用户数≥10000；支持各种操作系统的终端（安卓 10 以上、鸿蒙操作系统、Windows2000/XP/2003、Windows7/Windows8 32 位 64 位等系统）；支持用户静态超时退出功能；支持 SM1、SM2、SM3、SM4 商用密码算法和 RSA 公钥密码算法，传输内容采用 SM4 算法加密，不少于 8 套。

（2） VPN 集群 2:

VPN 集群：网络带宽支持万兆，需采用标准 SSL、TLS 协议提供虚拟隧道网络服务，提供基于 TCP、UDP、ICMP 等 IP 层以上的协议的应用服务；提供的 VPN 服务需要支持现有移动警务认证方式，包括但不限于 INSE 模式下国密 SM2 证书结合认证、SIM 卡贴膜卡国密 SM2 证书结合认证、SIM 卡贴膜卡商密 RSA 证书结合认证，支持伪装服务器地址功能，VPN 服务可以将真实的服务器地址伪装成域名形式。实现认证、访问控制、加密传输，并发用户数≥10000,4M 码流；VPN 网关拨号时间＜5S；接入用户数≥10000；支持各种操作系统的终端（安卓 10 以上、鸿蒙操作系统、Windows2000/XP/2003、Windows7/Windows8 32 位 64 位等系统）；支持用户静态超时退出功能；支持 SM1、SM2、SM3、SM4 商用密码算法和 RSA 公钥密码算法，传输内容采用 SM4 算法加密，不少于 4 套。

（3） VPN 集群 3:

VPN 集群：网络带宽支持万兆，需采用标准 SSL、TLS 协议提供虚拟隧道网络服务，提供基于 TCP、UDP、ICMP 等 IP 层以上的协议的应用服务；提供的 VPN 服务需要支持现有移动警务认证方式，包括但不限于 INSE 模式下国密 SM2 证书结合认证、SIM 卡贴膜卡国密 SM2 证书结合认证、SIM 卡贴膜卡商密 RSA 证书结合认证，支持伪装服务器地址功能，VPN 服务可以将真实的服务器地址伪装成域名形式。实现认证、访问控制、加密传输，并发用户数≥10000,4M 码流；VPN 网关拨号时间＜5S；接入用户数≥10000；支持各种操作系统的终端（安卓 10 以上、鸿蒙操作系统、Windows2000/XP/2003、Windows7/Windows8 32 位 64 位等系统）；支持用户静态超时退出功能；支持 SM1、SM2、SM3、SM4 商用密码算法和 RSA 公钥密码算法，传输内容采用 SM4 算法加密，不少于 2 套。

2. 通道保护网关

提供通道保护网关服务 1：单通道并发连接数不低于 1000 条/秒，每秒事务数不低于 1500，平均吞吐量不低于 800Mpbs,网络接口：千兆电口不低于 6 个，千兆光口不低于 2 个；支持强身份认证机制：可通过数字证书作为设备凭证，保证通道保护网关客户端和通道保护网关之间传输数据的机密性、完整性；支持终端数字证书注册，只有注册过并通过认证的可信终端才允许和安全网关之间建立安全链路，建立安全链路之后，可以通过安全策略自动中断终端和非可信网络之间的一切链路；应用服务接入到通道保护

网关后，保护应用服务与外部链接的逻辑隔离。要求支持冗余，不低于 3 套。

提供通道保护网关服务 2：单通道并发连接数不低于 5000 条/秒，每秒事务数不低于 1500，平均吞吐量不低于 8000Mpbs,网络接口：千兆电口不低于 6 个，万兆光口不低于 2 个；支持强身份认证机制：可通过数字证书作为设备凭证，保证通道保护网关客户端和通道保护网关之间传输数据的机密性、完整性；支持终端数字证书注册，只有注册过并通过认证的可信终端才允许和安全网关之间建立安全链路，建立安全链路之后，可以通过安全策略自动中断终端和非可信网络之间的一切链路；应用服务接入到通道保护网关后，保护应用服务与外部链接的逻辑隔离。要求支持冗余，不低于 2 套。

**3. 前置服务**

**（1） 前置服务 1**

支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 4096 张，单表数据影射最大字段数不低于 256 个，数据库到数据库交换记录数不低于 10000 条/秒，最大数据文件不低于 40G，并发客户端数量不低于 30000 个；支持网络带宽不低于 10G,提供不少于 2 套前置服务。

**（2） 前置服务 2**

支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 4096 张，单表数据影射最大字段数不低于 256 个，数据库到数据库交换记录数不低于 6000 条/秒，最大数据文件不低于 30G，并发客户端数量不低于 5000 个；支持网络带宽不低于 1G,提供不少于 8 套前置服务。

**4. 后置服务**

**（1） 后置服务 1**

支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修

改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 4096 张，单表数据影射最大字段数不低于 256 个，数据库到数据库交换记录数不低于 10000 条/秒，最大数据文件不低于 40G，并发客户端数量不低于 30000 个；支持网络带宽不低于 10G,提供不少于 2 套后置服务。

**（2） 后置服务 2**

支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 4096 张，单表数据影射最大字段数不低于 256 个，数据库到数据库交换记录数不低于 6000 条/秒，最大数据文件不低于 30G，并发客户端数量不低于 5000 个；支持网络带宽不低于 1G,提供不少于 8 套后置服务。

**5. 负载均衡服务**

要求吞吐量不低于 40Gbps，并发连接数不低于 8000 万次，满足设备冗余；支持轮询、加权轮询、按主机加权轮询、优先级等算法；具备支持源 IP 等多种会话保持机制，具备跨虚拟服务的会话保持机制、具备将服务器负载状态投屏展示能力，千兆电口不低于 4 个，千兆光口不低于 4 个、万兆光口不低于 4 个，要求光模块满配。至少提供 2 台。

### 2.3.3.2 公安信息网隔离交换服务需求

根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

**1. 提供负载均衡服务**

要求吞吐量不低于 40Gbps，并发连接数不低于 8000 万次，满足设备冗余；支持轮询、加权轮询、按主机加权轮询、优先级等算法；具备支持源 IP 等多种会话保持机制，具备跨虚拟服务的会话保持机制、具备将服务器负载状态投屏展示的能力，千兆电口不低于 4 个，千兆光口不低于 4 个、万兆光口不低于 4 个，要求光模块满配。至少提供 2 台。

**2. 提供交换服务**

提供交换服务，单台交换容量不低于590Gbps；包转发率不低于190Mpps；千兆电口不低于48个，能够实现设备堆叠，满足设备冗余。

提供交换服务，单台交换容量不低于4.8Tbps；包转发率不低于2000Mpps；万兆光口不低于48个，满配万兆多模模块，40G光口不低于4个，满配40G多模光模块，能够实现设备堆叠。

**3. 提供网闸服务**

基于HTTPS安全协议的管理方式；支持SYSLOG协议；支持SNMPX协议；对应用服务器进行设备认证，并对数据格式和内容检查；支持TCP/IP方式传输数据；文件同步功能，支持文件的同步，多级目录结构同步，可进行文件过滤；FTP同步方式，可支持30Gb大文件传输；数据库同步，支持触发器、全表、删除原表数据、时序等同步方式；千兆电口不低于6个，背板带宽不低于4Gbps，TCP/IP实际传输速率不低于800Mbps；数据库同步每秒不低于4000条；文件摆渡方式每秒不低于80Mbps，要求提供不少于8套网闸服务。

**4. 提供网闸服务**

基于HTTPS安全协议的管理方式；支持SYSLOG协议；支持SNMPX协议；对应用服务器进行设备认证，并对数据格式和内容检查；支持TCP/IP方式传输数据；文件同步功能，支持文件的同步，多级目录结构同步，可进行文件过滤；FTP同步方式，可支持30Gb大文件传输；数据库同步，支持触发器、全表、删除原表数据、时序等同步方式；千兆电口不低于6个，万兆光口不低于2个，背板带宽不低于10Gbps，应用层传输速率不低于8Gbps；数据库同步每秒不低于4000条；文件摆渡方式每秒不低于80Mbps，要求提供不少于2套网闸服务。

### 2.3.4 公安信息网安全服务需求

#### 2.3.4.1 公安信息网基础服务需求

公安信息网基础服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

1.提供核心交换服务，要求单台交换容量不低于206Tbps，要求包转发不低于38400Mpps，单台设备的主控、电源要求冗余，40G光口不低于24个，40G万兆多模光模块不低于4个，万兆光口数量不低于68个，万兆多模光模块满配，千兆光口数量不低于48个，千兆多模光模块满配，千兆电口不低于48个，要求设备冗余。

2.提供管理接入交换服务：要求单台交换容量不低于590Gbps；包转发率不低于190Mpps；千兆电口不低于48个，万兆光口不低于4个，配置不低于4个万兆多模光模块，能够实现设备堆叠，数量不低于8台。

4.提供负载均衡服务，要求吞吐量不低于40Gbps，并发连接数不低于8000万次，满足设备冗余；支持轮询、加权轮询、按主机加权轮询、优先级等算法；具备支持源IP等多种会话保持机制，具备跨虚拟服务的会话保持机制、具备将服务器负载状态投屏展示的能力，千兆电口不低于4个，千兆光口不低于4个、万兆光口不低于4个，要求光模块满配。至少提供2台。

6.提供堡垒机服务，需提供不少于50个支撑资源授权服务，需提供通过多种协议的服务，如字符协议SSHv1、SSHv2、Telnet，图形协议：RDP、VNC，文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板等；持图形协议并发支撑数不少于300个，支持字符协议并发支撑数1500个。可提供支撑人员单点登录、用户权限细粒度授权及访问控制、支撑过程审计等功能，提供从Web页面设置多端口绑定服务。

移动警务应用支撑服务根据2016年移动警务总体建设技术方案以及全国公安移动警务升级改造建设任务书要求，提供移动警务应用支撑服务，面向全局的移动应用开发提供支撑能力，辅助开发者在满足规范的要求下，获取全局的共享资源，快速低成本地进行个性化的应用开发。

所提供的所有的服务系统都需遵循统一的研发规则，规则包括且不仅限于如下：

1.大文件的跨网同步，必须通过文件摆渡的服务，不能使用接口服务形式。

2.所有应用都必须对接集中管控服务，按照应用日志的对接标准实现业务应用的日志实时上报。

3.所有服务涉及组织机构和用户信息的都必须与基础用户服务对接，根据基础用户服务提供的权限使用用户信息。

### 2.3.5 移动互联网区应用支撑使用服务需求

提供统一的互联网应用安全管理服务，支持对互联网应用的注册、发布、版本管理、检索、更新、下架、统计等全生命周期管理和日常的应用数据采集。

#### 2.3.5.1 统一安全门户需求

与互联网安全服务基座集成，实现统一的应用门户，统一应用入口。

提供统一的互联网服务运行门户，集成实名认证服务和身份认证服务，对接入移动互联网区域的应用进行身份认证，同时提供基于沙箱的安全运行环境，对运行的应用和

数据进行安全隔离，提供水印服务，对应用的运行桌面进行水印。

提供移动互联网应用管理服务，支持原生应用和轻应用的管理和部署下发。

#### 2.3.5.2 统一认证需求

提供实名认证服务，依托内网的实名认证服务或者自建的实名认证服务对Ⅰ类区用户群体进行身份实名核验，实名认证服务提供包括身份证号和姓名两要素、终端信息的认证服务，确保用户身份的合法性。

#### 2.3.5.3 服务总线需求

提供统一的服务资源管理，按照《移动警务服务总线技术参考指南》、《移动警务服务总线技术要求》和《移动警务应用支撑体系技术方案》等规范建设Ⅰ类区的服务总线。服务总线负责实现Ⅰ类应用服务端与Ⅱ类区数据或服务资源之间的请求调用、寻址、资源调度、权限控制等能力。服务总线负责实现服务的跨网调度，实现服务转换、注册、授权、访问控制和监控，与集中管控和公安部总线对接。

### 2.3.6 联网服务区应用支撑使用服务需求

#### 2.3.6.1 终端侧服务需求

##### 2.3.6.1.1 自定义门户服务需求

在单警应用支撑终端、移动警务办公终端负一屏集成自定义门户，支持集成卡片、元服务、原生应用的统一入口，实现终端系统账号与统一认证的打通。

终端人脸识别登陆系统模式与统一认证服务打通，实现强绑定认证。区分终端登陆模式与其他认证方式进入终端后的权限级别，人脸识别通过认证后系统进入已认证状态；其他登陆方式使用移动应用需要进行二次认证。

要求所提供的移动终端上预置自定义门户，门户中可灵活配置基础服务组件。要求在终端开通后默认可使用以下服务内容，包括但不限于：

1. 整合消息中心、预警中心、任务中心服务能力。

2. 整合元服务能力，包括：签到、热线等。

3. 整合卡片服务能力，包括：人工智能助手、图传、视频会议、打卡、日历、警务新闻、规范条例等。

4. 整合系统功能，包括：扫一扫、首都公安、首都警务报道、云盘等。

5. 支持不少于6万终端的使用需求，要求门户打开时间不高于3秒。

#### 2.3.6.1.2 泛终端智能协同服务客户端组件需求

##### 2.3.6.1.2.1 提供移动服务总线服务

升级移动警务服务总线，实现泛终端接入和终端能力的统一管理和服务。

泛终端智能协同服务客户端组件是实现“边、端侧”服务资源的统一管理和调用的核心能力，需同时满足移动警务智能终端、边缘网关、扩展类终端上服务资源的授权和调用管控，同时可以获取边端侧服务能力，实现从南向提取网关和终端的服务能力面对业务提供服务，实现支持物联网终端和网关服务能力自身开放的业务服务能力的统一接入管理和对外访问授权。

提供支持网关端和终端端部署实施的形式。支持对边缘网关、扩展类终端上的业务调用的分级授权需求。

以下是对移动服务总线的具体服务能力的需求：

1. 整合第三方 SDK 形式服务以及终端的能力，支持 SDK\APK 等不同形式的服务接口接入。包括且不仅限于光学识别组件、动态人脸识别服务组件、二维码服务组件、NFC 服务组件等。

2. 提供第三方 SDK 提供的业务服务能力，实现光学识别、人脸识别等服务。

3. 支持多应用类型接入服务，支持原生应用和基于 H5 的轻应用的调用。

4. 支持不限应用数量和应用类型的服务，支持不少于 6 万终端的服务需求。

##### 2.3.6.1.2.2 提供泛终端协同服务

提供泛终端协同服务，实现泛终端接入和终端能力的统一管理和服务,支持不少于 11 万终端的服务需求。要求泛终端协同服务及其包含的组件都支持安卓、鸿蒙等操作系统。

泛终端智能协同服务客户端组件是实现“边、端侧”服务资源的统一管理和调用的核心能力，需同时满足移动警务智能终端、边缘网关、扩展类终端上服务资源的授权和调用管控，同时可以获取边端侧服务能力，实现从南向提取网关和终端的服务能力面对业务提供服务，实现支持物联网终端和网关服务能力自身开放的业务服务能力的统一接入管理和对外访问授权。

提供支持网关端和终端端部署实施的形式。支持对边缘网关、扩展类终端上的业务调用的分级防控需求：

1. 提供消息服务组件，支持不同类型终端上的消息提醒能力，包括且不仅限于系统推送、弹窗、终端振动、信息提醒、语音呼叫、短信、电话呼叫等形式。

2. 提供终端组网服务组件，支持基于统一账户的设备靠近自动组网，支持 WLAN 和蓝牙。

3. 提供账户中心和基于账户的统一认证服务，并根据不同认证模式面向应用提供基于证书的统一认证、基于用户名密码、警号等多模式的认证形式。

4. 提供终端侧服务调用的鉴权控制服务，支持对终端服务、终端与终端之间的组网、设备访问之间的权限控制，并面向设备和应用提供统一鉴权服务。

5. 集成终端安全管控、证书管理服务，实现设备终端行业标准化接入。

6. 综合定位服务组件：整合 LBS、北斗定位、高精定位多种定位方式融合的客户端综合服务定位能力。

7. 移动音视频客户端组件：提供音视频客户端服务组件，支智能语音客户端组件：提供语音转写、合成等智能语音客户端的服务组件能力。

8. 授权组件：支持对终端侧网络接入、连接、组网和服务调用的授权转发。

#### 2.3.6.1.3 空中发证服务需求

提供空中发证服务支持对证书的远程管理，满足公安部下发的《全国移动警务 PKI 空中发证技术方案》要求。支持不少于 11 万终端的服务需求。

空中发证服务需结合位于公安信息网的移动警务 PKI 系统和终端的密码模块，实现高效的移动警务证书管理。

支持用户端自主发起证书操作请求以及服务端远程操作证书。

提供基于生物识别或者 PIN 码的用户认证，与移动警务 PKI 系统通信实现证书的各项管理功能。

提供多类型终端证书的管理和发证服务，支持鸿蒙、安卓、嵌入式终端的证书发放。

### 2.3.6.2 边缘侧服务需求

升级边端应用支撑和管理服务，实现支持泛终端协同服务边缘侧服务能力。支持不少于 20 终端的并发接入。

#### 2.3.6.2.1 边缘终端接入管理服务

根据警用无线局域网总体技术方案要求，采用 PWL 专用传输链路实现扩展类终端接入移动警务网。

提供对网关入网、终端入网的安全网络接入、设备分组管理、设备发现等服务能力。

支持与现有云端终端管控服务能力对接满足对入网终端和网关的安全管控。提供相关技术标准，满足接入不同终端的管控和服务系统。支持对设备的管控能力进行转换，

面向业务提供相关服务。

满足公安部边、端协同有关标准，提供边、端协同扩展类终端安全接入管理服务，支持注册、发现、登录、注销、遥晕、遥开、遥闭等功能。

提供边、端协同终端统一身份识别服务，按公安部有关标准制定终端唯一身份码，包含设备操作系统、通信机制、管理或使用人员等信息。

支持与移动警务证书系统对接服务，依据证书核验结果实现对终端的接入控制。

提供对网关型终端、扩展终端等设备状态的管理服务，支持对物联设备状态、分组、是否在线等信息的管理。

提供网关型终端、扩展终端数据上报和控制指令下发的转发能力、支持数据断点续传。

支持采用手动或自动方式对设备进行安全分级，实现设备安全互联。

提供设备分组与组权限管理服务，支持根据管理及使用需求对多设备进行设备组建立/删除、添加/删除组内设备，支持对网关型终端设备分组功能权限管理，实现对多设备群组化使用和管理。

提供基本管理服务，包括且不仅限于设备组成员管理，协同资产管理服务、安全审计服务、策略管理转发及跟踪服务。

提供群组设备访问控制服务，建立设备间信任环机制，支持设备间安全访问及数据传输。

按照公安部边、端协同有关标准，提供边、端协同功能配置接口，满足各类用户管理和配置要求。

支持移动警务集中管控中心相关要求，提供边、端协同服务管控接口，满足移动警务集中管控需求。

提供符合公安部边、端协同有关标准要求的网关终端安全监控服务接口，满足对不同网关终端进行安全监控的需求。

支持异常场景自动恢复服务，解决用户在实际使用中，因为异常操作、设备异常断电、程序卡死等出现的异常场景自动恢复功能。

提供网关型终端报表统计服务，支持终端用户统计、设备统计、安全统计、网络统计等报表。

支持对网关管理权限的配置，包括且不仅限于安全监控能力管理权限、管控策略调整和分发服务。

提供支持不同类型的终端、不同类型的操作系统上的应用的边缘服务调用需求进行管理和管控，并根据集中管控的技术标准实时上报资源服务使用状态。

支持提供配置，实现服务运行数据在网关端、终端侧的二级缓存和上报。

#### 2.3.6.2.2 边缘算力网络管理

提供通过动态自治组网连接分布各处的端设备，和面向边端协同的资源虚拟化技术，构建层次化算力感知图。

提供通过多粒度多层次的资源调度与跨空间的算力协同等服务能力，充分利用端侧设备能力，为端侧用户就近提供充足的资源处理能力和广泛的设备交互能力。

提供任务管理服务，任务管理可以从服务市场选择所需部署服务用，部署到指定集群；服务部署可以指定某个或多个（全部）集群；由该集群管理面负责分配到可适配的服务的工作节点上；若所选集群无满足服务要求的工作节点，则产生提示信息；若所选集群中部分集群工作节点不满足任务信息，则产生提示信息，满足条件的正常部署。

提供集群任务管理服务，支持任务列表的显示范围为某一指定集群内（包括该集群挂载的云资源、该集群挂载的其他集群）部署的任务；支持异常任务管理和任务详情的展示。

提供集群管理服务，支持集群的创建、维护、查看以及集群的状态监控。

提供设备管理服务，支持对设备的接入控制、发现、状态监测。

提供算力服务管理服务，支持维护算力服务和算力资源的使用行为统计；支持多账号和集群管理，可以创建任意多组织账号和角色，并针对性进行权限管理。

提供支持云端集中式算法调用模式，接入第三方云端算法服务，提供面向任务实时调用的方法。

提供支持单算法服务容器动态扩容的方式，根据单算法服务使用资源情况进行动态扩容和动态删减资源。

提供支持预计算算力资源统一部署的模式，根据算法和任务对算力资源的需求，结合实际使用需求，动态计算算力资源设备，实现服务的动态部署能力。

### 2.3.6.3 云端运行支撑服务

#### 2.3.6.3.1 资源管理服务需求

移动警务资源管理服务是移动警务服务资源和算力资源统一管理的服务，在新任务书和技术规范的要求上，需新增扩展类终端、网关型终端对服务资源的调度控制，作为统一的服务控制中心，需同时满足移动警务智能终端的上业务应用、边缘网关业务服务、

扩展类终端上业务应用对中心端资源获取时的授权和管控措施，同时在原有云资源服务统一北向调用防控的基础上，与边、端资产接入和管理服务进行整合，支持从南向提取网关和终端的服务能力以及管控能力。北向面对业务提供服务，实现支持物联网终端和网关服务能力自身开放的业务服务能力的统一接入管理和对外访问授权。

提供支持不同类型的终端、不同类型的操作系统上的应用的调用需求进行管理和管控，新增网关部署服务资源的使用需求，并根据集中管控的技术标准实时上报资源服务使用状态。

提供支持云端服务、网关端服务的接入和管控能力，网关端服务面向接入终端提供、云端服务面向网关和网关上的接入终端提供服务。

支持云端部署和边缘网关部署的形式，通过云、边联动实现对边缘网关、扩展类终端上的业务调用的分级防控需求。

支持提供配置，实现服务运行数据在云端、网关端的二级缓存和上报，支持根据配置实现边、端服务信息的层级上报和直连上报模式。

支持视频类、实时消息类服务的管理和访问授权，支持跨网的安全调度。支持且不仅限于 RTSP、RTMP、SIP、GB/T 28181 等音视频协议，支持在跨网过程中实现地址转换的编解码，实现音视频流的无缝地址转换。视频类权限的控制包括对第三方接入平台的授权控制、对使用对象的访问控制等形式。

提供针对全局所有的开发服务资源的统一管理和对外共享服务，实现资源的可管控，可共享，包括服务总线和移动服务总线。

提供包含基于服务端的服务总线以及客户端的移动服务总线，服务总线实现数据资源接口的管理和共享，移动服务总线服务面向客户端集成的 SDK 等服务进行协议转换，面向全局轻应用和安卓原生应用提供调用和管理服务。

提供服务统一管理能力，实现服务总线和终端集中能力资源的统一维护、授权，并通过服务总线和移动服务总线实现对外共享服务。

要求完成原有移动警务应用的服务资源接口的接入工作，实现原有应用使用的平滑过渡。

与公安部资源服务子平台对接，实时上报服务资源的具体内容以及数据资源服务的调用情况。

提供不限应用数量的支撑能力、并发服务能力不得低于 1500 次/秒，终端同时在线数量不得低于 11 万，响应时间不得超过 3 秒。

### 1. 统一资管理服务

统一管理服务提供对总队业务服务、公安信息网数据服务、通用组件服务的统一管理，提供服务协议的转换，服务目录的注册、检索与展示，服务申请审批、授权、访问控制和监控。

统一管理服务提供系统运行监控可视化展示等管理能力。

统一管理服务提供服务在线注册（包含批量导入注册）、注册审核、注册历史记录等服务注册管理能力。

统一管理服务与用户服务对接，定时同步机构信息，提供全局用户 ID 统一生成的服务能力。

统一管理服务提供服务授权申请、审核、历史授权服务查询、有效授权信息导入导出、服务授权维护等管理能力。

统一管理服务提供服务目录编制、服务目录状态查询、服务目录发布、服务信息自动发现、多维度服务目录展示（包含且不仅限于应用维度、分局维度、类别维度、操作维度、警种维度）、服务目录全文检索能力。

统一管理服务提供服务状态的变更管理、自身服务启停状态控制管理、自身应用接口变更管理能力。

统一管理服务支持数据推送服务，支持异构数据库之间的数据推送、文件数据导入能力、文件格式管理能力、目录扫描导入能力、数据内容导出能力等数据接入服务。

统一管理服务提供资源管理自身的日志缓存处理、报文转存处理、日志批量入库、推送、查询、检索、导入导出等日志服务能力。

支持资源服务目录与开发者支撑进行同步。

统一管理服务提供用户信息、服务注册信息、服务使用信息等统计分析报告，包含且不仅限于服务调用量统计、分局统计、业务应用统计等不同数据分析维度。

支持视频类资源的统一维护管理。包括音视频地址流的管理、音视频流格式的配置，音视频内容的管理。

支持对音视频流调用方应用的配置、调用方用户信息的配置，以及支持对相关调用方的权限配置，要求权限配置细化调用方对流地址的控制、对流内容的控制。

### 2. 服务总线

提供公共和私有两种校验方式的独立报文校验、报文格式校验、请求权限校验、异常报文识别服务、异常报文处理和反馈能力、非授权请求的反馈能力、权限访问控制能

力等管理服务。

提供接口和视频、消息等服务资源的请求、协议转换、调用、异常访问控制、请求报文的采集、响应报文的采集能力。

与智能应用开发服务对接，提供资源服务。

提供在移动互联网、联网服务子平台和公安信息网服务子平台的服务能力，分别为Ⅰ、Ⅱ、Ⅲ类应用提供服务,并通过服务接口方式互联互通，以实现对不同环境的移动警务应用提供基础支撑。

提供满足所有类型的数据资源格式的接入（包括不仅限于：Webservice、Json、http、https 等），面向前端应用提供统一的调用服务接口。

要求服务总线的数据类转发性能不低于 1 秒，支持同时访问并发不低于 500 次/秒。

要求服务总线对音视频流的转发性能满足以下标准：本网流纯转发、编解码的流转发、跨网的流转发能力不高于 1 秒。纯流转发能力不低于 3000 路并发，跨网流转发能力不低于 1000 路转发。

与集中管控对接，上报移动服务总线资源的使用情况，包括：调用频率、授权结果、异常信息等

#### 2.3.6.3.2 泛终端智能协同云服务需求

##### 2.3.6.3.2.1 泛终端物联服务需求

###### 2.3.6.3.2.1.1 多协议接入服务

提供终端接入通讯协议标准，支持 mqtt\http\tcp\coap 等主流通信协议，满足设备使用标准协议快速接入的需求。

提供自定义协议适配插件管理服务，支持第三方协议设备快速通过自定义协议接入平台，自定义协议支持 mqtt\http\tcp\coap 等主流通信协议。

提供自定义协议插件包的服务管理能力，支持第三方插件包在平台上的可视化管理，包括且不仅限于端口管理、服务启停、负载分布等能力。

提供设备快速接入的技术规范和平台测试环境，支持第三方设备快速进行接入适配。

提供泛终端连接状态的管理，支持状态同步给第三方系统，同时可对设备的连接状态进行管理，包括且不仅限于查询、断开等操作。

###### 2.3.6.3.2.1.2 泛终端认证

提供多种终端认证机制，支持密钥认证、证书认证、Token 认证等主流认证方式，满足不同安全等级设备的认证接入需求。

提供动态密钥管理服务，支持第三方系统通过标准接口为设备生成临时访问凭证，实现安全可控的短期接入授权。

提供终端嵌入式认证服务组件，支持多类型终端的快速接入认证。

提供自定义认证插件管理能力，支持第三方认证逻辑以插件形式接入平台。

提供认证凭证的生命周期管理，支持对设备证书、密钥等凭证进行全流程管理，包括且不仅限于颁发、吊销、更新、校验等操作。

提供设备认证状态的可视化监控与管理，支持实时查看设备认证成功/失败状态，并可将认证结果同步至第三方业务系统。

#### 2.3.6.3.2.1.3 数据和服务标准化服务

提供标准物模型定义与管理能力，支持设备属性、服务、事件等数据模型的自定义建模，确保各类终端数据按统一规范接入平台。

提供基于物模型的数据解析与验证服务，支持设备上报数据按物模型定义进行自动解析与校验，确保数据格式和内容的标准化。

提供基础数据类型支持，包括但不限于整型、浮点型、布尔型、字符串、枚举类型、时间戳等基本字段类型，满足各类终端数据的标准化定义需求。

提供复杂数据结构定义能力，支持数组、列表、键值对等集合类型，允许在物模型中定义和使用这些复杂结构，以适应多样化数据场景。

提供对象嵌套定义功能，支持子对象多层嵌套定义，允许在属性、服务参数等场景中使用嵌套对象结构，实现复杂数据模型的精准描述。

提供结构复用与继承机制，支持物模型之间的继承关系定义，允许通过扩展基础模型创建新的物模型，减少重复定义，提升模型开发效率。

提供数据类型验证规则扩展，支持为各字段类型添加自定义验证规则，包括取值范围、字符串格式、数组长度等约束条件，确保数据有效性。

提供向后兼容的模型变更管理，支持在保持向前兼容的前提下对字段类型和结构进行扩展，确保物模型迭代不影响已有设备和业务系统的正常运行。

提供物模型驱动的数据路由与转发能力，支持将设备数据按物模型维度路由到不同第三方系统，并保持数据格式的一致性。

提供物模型服务接口对外开放，支持第三方系统通过标准 API 订阅设备数据、调用设备服务及查询设备状态，实现跨系统数据交互。

提供物模型变更管理与版本控制，支持物模型定义的迭代更新与历史版本兼容，确

保业务系统数据接口的稳定性。

#### 2.3.6.3.2.1.4 规则引擎服务

提供灵活可配的规则链设计能力，支持通过可视化配置方式定义数据处理逻辑，实现数据过滤、转换、富集与分发等多种场景。

提供丰富的规则触发条件，支持基于设备上下线事件、设备属性上报、设备事件触发等多种条件启动规则执行，满足实时响应需求。

提供强大的数据处理与动作执行能力，支持 SQL 表达式、JavaScript 等语法进行数据解析与计算，并可触发向消息队列、数据库、第三方应用等多种目标的消息转发与指令下发。

提供规则引擎对外服务接口，支持第三方系统通过 API 对规则进行创建、启停、更新与监控，实现规则生命周期与业务系统的联动管理。

提供规则引擎的高可用与负载均衡支持，确保海量设备数据下的高吞吐与低延迟处理，并具备水平扩展能力以应对业务增长。

提供规则执行状态的实时监控与日志服务，支持对规则处理量、成功/失败率等关键指标进行可视化展示，并将异常结果同步告警至指定方。

#### 2.3.6.3.2.1.5 统一消息服务

提供统一消息服务，满足移动警务消息推送的统一管理与调度，并实时接收和记录目标端对消息的接收反馈。

支持跨网络域、跨应用系统的服务模式，确保消息在复杂环境下的可靠触达。

提供可维护的消息模板库，支持按业务场景预置多种格式模板；模板内容支持变量占位符，实现消息的个性化与动态填充。

提供多信道消息分发能力，支持通过邮箱、终端推送、Kafka、MQTT、HTTP 等多种渠道发送消息，并根据策略自动选择或同时启用多个通道。

消息推送到达率不低于 99.9%，端到端响应时间不高于 3 秒，确保高可靠与低延迟。

支持并发服务不低于 500 次/秒，并可根据业务负载动态调整资源，实现弹性伸缩。

提供智能终端及多种物联网终端的消息推送能力，覆盖主流终端类型。

支持文本、多媒体文件、URL 链接等多种内容形式的推送。

与资源管理系统对接，对外开放服务接口，便于第三方系统集成与调用。

提供统一消息保活与重试机制，确保在网络波动等异常情况下仍可完成消息投递。

支持不限应用数量的服务接入，具备一次性针对至少 11 万终端的大规模推送能力。

与集中管控服务对接，按照审计标准实时提交消息发送、投递及反馈等全流程日志数据。

#### 2.3.6.3.2.2 音视频融合服务需求

以泛终端物联服务的资产和授权管理服务为基础，针对音视频设备的音视频能力服务进行延伸，提供音视频整体服务能力。

**1. 融合通信服务**

为每个派出所、交通支大队、直属总队提供音视频网关服务，包含视频会议服务和流媒体调度服务，不少于 550 套以及 8%的备机服务。音视频网关服务要求：处理器不低于 8 核，运行内存不低于 16GB，存储空间不低于 64GB，视频支持 H.264/H.265 编码及 H.265、H.264、AV1、VP9、AVS2 解码，支持 1080P 分辨率，音频具备自动回声消除、自动增益控制、自动噪声抑制与唇音同步功能；配备不低于 7 路音频输入、6 路音频输出、4 路视频输入、3 路视频输出接口，集成多规格 3 个 USB 及 2 个 RJ45 网络接口；适配 0℃-40℃工作温度，具备工信部入网许可证、CQC 认证。支持泛终端管控组件适配要求。

融合通信平台对外提供的服务能力以 WebSDK、安卓 SDK、鸿蒙 SDK 和 API 四种形式提供，主要面向 Web 应用开发、安卓应用开发、鸿蒙应用开发三种模式。

融合通信能力服务平台作为应用支撑的能力部分，支撑其他第三方指挥类业务，打通多端指挥业务的互联互通。

对外提供的服务内容包括：视频会议融合、语音对讲融合、短信服务、电话外呼服务等，其中：

- 视频融合：支持现有多种视频流的融合，包括图传流、移动视频会议流、内网非涉密会议系统以及固定监控、无线监控、VoIP 电话等形式的音视频流的融合，
- 提供视频融合基础服务能力，提供基于 WebSDK 和安卓 SDK 以及 pc SDK 的形式，包括会议发起、会议预约、会议录制、会议控制、多源视频接入等能力。
- 语音对讲：支持 800M、1.4G 和 350M 语音平台的互联互通，打通对讲服务，并对外提供基于 WebSDK 和安卓 SDK、pc SDK 的形式对外提供，包括单呼、组呼、创建虚拟组等服务能力。
- 集成 P-POC（公网对讲）服务，实现平台与移动警务平台联动,通过平台对接从而实现公网对讲与移动警务、PDT 专网的三网打通，实现异构网络互通，实现民警、协辅警等不同形态、不同制式终端的统一调度。
- 监控调度：包括视频监控资源同步、视频流播放、视频编辑工具等服务。

- 无线图传：与音视频服务能力对接，整合服务资源，以 WebSDK、安卓客户端 SDK、API 的形式面向应用提供服务，主要包括：图传资源的同步、图传状态同步、图传发起、图传流调取等服务。
- 短信服务：提供 API 短信网关，提供支持跨网的短信发送业务，包括点对点、群组短信、短信回执、定时短信等服务。
- 电话外呼服务：提供基于 WebSDK、安卓客户端 SDK 的形式提供电话外呼服务，支持中心节点呼叫普通移动号码、固定电话号码。

**2. 移动音视频服务**

开放终端开发能力服务，与资源管理服务系统对接，开放所有服务端能力。

对接各种监控平台视频源，实现监控的接入。

与集中管控服务对接，按照集中管控应用日志的标准实时上报使用日志。

对外开放的服务支持不限应用数量的调用服务，支持 11 万终端的使用。

**（1） 客户端服务需求**

视音频流媒体服务主要面向市局各类应用厂商，提供视音频业务的快速应用开发和上线能力，提供视频回传、图传互动、视频点播、视频拉取等业务场景。通过配置应用服务，在应用客户端快速集成 SDK，即可获得面向业务的视音频业务功能。

视音频流媒体服务功能包含端侧服务和云侧服务两方面。端侧服务应为市局各应用厂商提供高度集成化的 SDK 功能模块，以快速实现视音频业务的开发及上线。云服务提供云端服务能力支撑。

**（2） 端侧服务功能需求**

端侧服务功能需满足安卓、鸿蒙等操作系统的要求。

- **终端侧视音频回传 SDK**

终端侧视音频服务 SDK 应支持高清视音频回传、视音频缓存回传、点调回传、视频源控制、视音频录制等功能。

终端侧视音频服务 SDK 应支持设置回传视频清晰度，最低分辨率 480×270，最高分辨率可达 1080P，最大码率支持 4M，视频回传协议统一采用 RTC 协议，支持带宽自适应，支持画质优先、流畅度优先和质量自平衡等策略，在网络条件差的情况支持确保音频流畅。

终端侧视音频服务 SDK 功能应包含：

支持实时回传、延时回传和历史文件回传三种模式。

回传参数要求如下：

- 视频回传视频分辨率支持 1080p、720p 两种模式，码率分别支持 2M-4M、500kpbs-2M。视音频回传帧率最高支持 30 帧。
- 回传视频应支持 H.264、H.265 的编码格式。

➢ **终端侧视音频调取 SDK**

终端侧视音频调取 SDK 应为第三方厂商开发者提供简单、快捷的接口，帮助开发者实现基于移动警务终端的视音频播放应用。

SDK 统一采用 RTSP 和 RTC 协议；支持软硬解码，支持 H.264/H.265 视频编码格式，支持截图及自动获取视频缩略图功能；支持纯音频播放、后台音频播放等功能。

➢ **视音频调取 WebSDK**

视音频调取 WebSDK 应为开发者提供支持浏览器播放 RTSP,RTC 协议的视频接口能力。SDK 应支持界面自适应缩放，支持 H5 和 flash 播放，支持 hls 直播。

➢ **终端互动播放 SDK**

终端侧互动播放 SDK 应为开发者提供互动播放视音频功能。SDK 应支持直播画面的启动、暂停和结束等播放控制功能，支持画面调整、屏幕截图等功能，支持直播视频连线功能。

➢ **互动播放 WebSDK**

提供互动播放视音频功能，SDK 应支持直播画面的启动、暂停和结束等播放控制功能，支持画面调整、屏幕截图等功能。

➢ **终端侧视频互动 SDK**

终端侧视频互动 SDK 以模块化接口形式提供给开发者进行业务集成，支持低延时互动、支持自定义分辨率、码率设置，支持软硬编解码。支持前后摄像头切换、本端与远端画面大小屏切换；支持点对多音视频互动、支持视频互动与纯音频互动转换。

**（3） 云服务业务功能服务**

云服务为终端端 SDK 模块提供平台级能力和相应的管理服务。

**（4） 流媒体平台服务需求**

支持多种级联方式，支持按照根据用户所属区域、统计负载接入，按照求对视频流进行前端直接转发，提供灵活的实现音频和视频的转发。

流媒体服务对设备的接入、认证、设备基础数据的获取都需经过统一的泛终端管理平台获取，并将接入设备的实时推流状态、在线状态、通道信息和流编码信息回推到物

联网平台和流媒体管理平台。

- **视音频接入需求**

流媒体接入网关应提供接口级的服务支撑能力，支持作为上级平台 RTSP、GB/T 28181、RTC 等协议的视音频流数据接入需求。

RTSP 协议网关支持主动拉流方式或被动推流两种模式，RTSP 协议视音频编码参数要求：

- 视频格式：H264、H265。
- 视频编码分辨率:1080p(1920x1080)720p(1280x720)、VGA(640x480) 。
- 视频编码帧率: 15-30 帧。
- 视频码率:0.5M~12Mbps。
- 音频格式：G711U、G729、AAC。
- 音频采样率：16k~320Kbps 。

GB/T 28181 接入网关需支持的视音频编码参数要求如下：

- 视频格式：H264、H265。
- 视频编码分辨率:1080p(1920x1080)720p(1280x720)、VGA(640x480) 。
- 视频编码帧率: 15-60 帧。
- 视频码率:0.5M~12Mbps。
- 音频格式：G711U、G729、AAC、PCM。
- 音频采样率：16k~320Kbps。

RTC 流媒体接入网关需支持的视音频编码参数要求如下：

- 视频格式：H264、H265。
- 视频编码分辨率:1080p(1920×1080)720p(1280×720)、540P（960×540）、270P（480×270）。
- 视频编码帧率: 15-30 帧。
- 视频码率:0.2M~3Mbps。
- 音频格式：G722、SILK、L16、OPUS
- 音频采样率：16k~48Kbps。

GB/T 28181 级联网关支持上级平台级对接，支持接受下级注册、注销，支持网络设备信息查询（设备目录查询、信息查询、状态查询）及设备控制（球机/云台控制、设备远程启动控制、强制关键帧控制、设备录像控制、图像放大/缩小），支持移动设备

位置订阅和通知。

支持基于 RTC 和 RTSP 提供互动视音频流接入，提供呼叫、应答、挂断、静音/取消静音、摄像头切换等能力支持。

支持通过 HTTP 方式进行 MP4、FLV、TS 等文件的单文件和批量上传功能，支持多线程快速上传能力。支持通过从第三方平台主动下载 TS 文件，支持重传和多线程下载，支持 M3U8 队列下载 TS 序列及自动合并 TS 文件。支持 TS 转码为 MP4 等格式的能力。

支持作为下级平台进行 GB/T 28181 和 RTMP 对接的能力，支持视音频流的状态管理和通知能力，支持上传视音频的元数据管理、防盗链及码率自适应能力。

- **视音频推送需求**

流媒体服务应支持通过 HTTP API 控制平台主动推送历史视音频文件、设备流、直播流给特定用户、平台，推送模式为 RTSP/GB/T 28181/RTC。

作为 GB/T 28181 下级平台对接时应支持主动向上级平台注册、注销的能力，支持网络设备信息查询（设备目录查询、信息查询、状态查询），支持设备控制（球机/云台控制、设备远程启动控制、强制关键帧控制、设备录像控制、图像放大/缩小），支持移动设备位置订阅和通知。

支持通过访问流媒体服务存储的 MP4、FLV 和 TS 文件，应提供批量导出和主动上传到对应位置。TS 文件存储分片处理生成 M3U8 点播列表，可选直接发布到 HLS 服务器进行历史视音频点播。

支持多路视音频流实时合成并主动推送到指定流媒体服务器，推送内容可录制。支持控制视频布局方式和合成后分辨率码率等。支持视频流的基础信息和状态信息查询功能。

支持流媒体服务底层通过频道订阅的模式，实现用户流之间的相互订阅，向上形成音视频互动、会议等多类型互动场景。

支持通过 GB/T 28181 协议向上级平台推送视音频流，支持虚拟设备 id 通过 Web 接口汇报给上级平台，供上级平台调取。

- **视音频直（点）播需求**

支持直播频道创建、上/下线，以及直播点播内容的分类管理功能。

支持通过 HTTP API 进行多类型点播、轮播等内容的列表查询功能。支持返回指定频道的播放地址列表。支持抽取内容图片功能。

支持通过 HTTP 方式进行视音频文件上传，需支持多种格式（MP4、TS、FLV、MKV

等），支持批量上传及多线程快速上传。支持视音频文件的点播播放，允许拖拽/快进操作。

支持直播点播内容的用户播放统计和报表展示功能。

支持双向实时音视频及纯语音互动功能，支持音视频互动文件录制功能，相关参数规格要求如下：

- 视频封装: MP4、TS、FLV。
- 视频格式：H265。
- 视频编码分辨率:1080p(1920×1080)720p(1280×720)。
- 视频编码帧率: 15～30 帧。
- 视频码率:0.5M～12Mbps。
- 音频格式：MP3、AAC 等。
- 音频采样率：16k～320Kbps。
- 视音频延时范围：0～60 秒。

➢ **视音频加工处理需求**

提供视音频全链路监测能力，支持从端侧接入环境到云端各节点的性能和使用情况的监测。

➢ **转码集群需求**

支持通过 HTTP API 实时转换 TS、RTMP 及 GB/T 28181 流媒体的能力；支持一进多出（同时转换出多路分辨率/码率、封装格式不同的视音频流）转换模式。支持通过 HTTP API 对 MP4、FLV、TS 编码视音频文件进行实时/闲时转码的能力。转码状态查询需求

支持通过 HTTP API 查询当前转码队列和转码文件状态。

支持用户配置转码模板，方便进行快速解码,参数需求如下：

- 视频格式 （MP4、FLV、TS/M3U8 分片）。
- 视频编码（H264、H265、SVAC）。
- 音频格式 （AAC、PCM、Speex、G711、G729）。
- 音频采样率：16k～320Kbps。

➢ **分布式存储需求**

支持分布式存储，需具备高性能、没有任何 I/O 热点、易管理、易维护、可计划性扩展，并可附加各种企业级功能的能力。

应支持用户读取数据时就近访问边缘的存储节点，实现高速访问。具备自动从中心

和周围节点复制数据块到边缘节点的能力。应支持某个存储节点数据损坏时，数据区块自动迁移，以保证数据安全。网络增加存储节点时，自动整体扩容存储容量和 IO 吞吐性能。

- **管理服务需求**

提供流媒体管理服务为管理员提供流媒体的查询、点播、录播等后台管理能力，同时支持配置业务权限及鉴权服务。支持设备信息管理、群组管理、对接视音频资源等资源管理功能。

需支持用户、设备、网络状态和流媒体平台运行日志、运行状态的统计和优化分析能力。

#### 2.3.6.3.2.3 AI 智能化服务需求

要求以下 AI 服务在满足自身业务能力的基础上，其中云服务需支持第三方智能体应用开发平台的调用需求，主要满足以下能力：

1. 暴露标准的 MCP 服务端点，支持工具注册和管理。
2. 提供工具调用接口，支持参数验证和执行结果返回。
3. 实现资源访问协议，支持数据资源的标准化读写操作。
4. 具备 prompt 模板服务，支持动态提示词管理和调用。
5. 提供服务发现机制，支持客户端自动识别可用能力。

##### 2.3.6.3.2.3.1 终端侧智能服务

终端侧智能服务要求支持安卓、鸿蒙等操作系统。

###### 2.3.6.3.2.3.1.1 光学识别组件

提供证件 OCR 识别服务，通过拍照、视频方式实现身份证、驾驶证、外国人护照、社保卡、军官证等各类证件信息的统一 OCR 动态识别。

提供车辆车牌 OCR 识别服务，通过拍照、视频方式实现车辆车牌号的 OCR 动态识别，采用文字识别（OCR）技术，自动提取车牌号信息（包括省简称、专用文字和大写英文及数字）。

提供车辆 VIN 码 OCR 识别服务，通过拍照、视频方式实现车辆车架号的 OCR 动态识别，采用文字识别（OCR）技术，自动提取车架号信息（包括大写英文及数字）。

支持复杂背景（如将证件拿在手中）裁边；支持自动倾斜校正功能，提高识别率。

提供印刷品识别服务印刷品识别服务应该支持拍照提取文档，上传附件提取文档，支持对文档内的文字进行提取形成电子版的服务能力。

提供数据上报服务，包括图片和使用日志。

支持不计数量的应用的接入服务，支持满足 11 万终端的使用需求。

与移动服务总线对接，开放所有服务接口。

与集中管控服务对接，按照应用日志接入标准要求实时上报服务的使用记录。

#### 2.3.6.3.2.3.1.2　动态人脸识别服务

**1. 客户端服务能力要求**

人脸检测与跟踪服务能力，支持检测图片或视频流中的人脸并返回人脸框，支持视频流中的人脸追踪。

实时视频流人脸检测抓取服务能力，支持输入实时视频流自动识别和截取人脸图片数据，并支持计算人脸特征值数据。

录像视频文件人脸图片抓取服务能力，支持输入录像视频文件自动识别和截取人脸图片数据，并支持计算人脸特征值数据。

图片抓取服务能力，支持输入一张或多张图片自动识别和截取人脸图片数据，并支持计算人脸特征值数据。

人脸特征库服务能力，支持不低于 5000 人脸特征库，并支持人脸特征库的增删改查等能力。

人脸检索能力，支持 1:1 比对和 1:N 以及 n：n 比对，1:1 比对支持输入两张照片进行比对，1:n 支持输入一张图片，与选定人脸特征库进行比对，返回超过阈值的人脸特征 ID。N:n 支持输入多张照片，与选定人脸特征库进行比对，返回超过阈值的人脸特征 ID。

支持最低 30 万像素摄像头格式，支持 NV21 BGR 图像格式。

与移动服务总线服务对接，面向全市开放服务能力。

支持不同类型的应用的对接，支持不少于 11 万终端的使用需求。

提供移动端人脸识别开发 SDK 包。

#### 2.3.6.3.2.3.2 云端智能服务

#### 2.3.6.3.2.3.2.1　动态人脸识别服务

需具备数据接入北京市公安局视频图像综合应用平台的能力。

需具备按照 GA/T 1400 标准与北京市公安局视频图像信息库数据调用能力。

需具备北京市公安局视图布控告警任务下发接收能力。

需具备北京市重点关注人员管控预警能力。

需具备北京市千万级人员聚类归档能力。

需支持 6000 张/秒比对的并发能力。

**1. 服务端服务能力**

人像解析:

人脸解析是自动检测并截取视频流或图片流中人脸，并分析获取人脸特征信息等。

解析中心支持实时解析、录像解析、文件解析能力。实时解析支持对在线相机新建单个或批量的实时分析任务实时解析，查看选定相机的分析结果和报警结果。

录像解析对历史录像新建单个或批量相机的结构化分析任务，查看选定任务分析结果和报警结果。

文件解析对上传的离线视频、图片、压缩包等文件新建结构化分析任务，查看任务详情、任务分析结果及任务报警结果。

人像检索:人脸检索能力，支持 1:1 比对和 1:N 以及 N:N 比对，1:1 比对支持输入两张照片进行比对，1:N 支持输入一张图片，与选定人脸特征库进行比对，返回超过阈值的人脸特征 ID。N:N 支持输入多张照片，与选定人脸特征库进行比对，返回超过阈值的人脸特征 ID。

人像比对:人像比对通过输入两张人脸照片，进行 1:1 比对，快速给出这两张人像图片的比对结果。

底库管理：底库管理主要维护人像基础底库。支持增删改查底库信息，支持增删改查底库名单，支持查看底库的名单详情，支持底库名单的批量管理。针对不同的服务对象，支持自定义底库目录。

对接视综服务能力：根据视频专网和公安信息网视综平台业务需要，移动信息网数据中心提供统一服务能力，将原始人脸抓拍数据、人脸识别服务平台解析后的人脸图片、特征值、属性信息等数据统一提供视频专网市局视图总库，供视频专网进行视频图像综合应用。

提供将视综预警信息接入移动信息网的能力。

服务端能力和视综对接能力需对接服务总线，并统一对方提供服务。

与资源管理服务进行对接，通过警务移动网络，将采集到的人脸数据实时回传至后台，最终数据汇总到市局视综平台。

提供与集中管控服务对接，按照应用日志接入标准要求提供文件传递的实时日志信息。

#### 2.3.6.3.2.3.2.2 智能语音引擎服务

提供不限应用数量的调用方式，满足 11 万终端的使用需求。

**1. 引擎基础架构**

智能语音引擎服务面向开发者提供底层的引擎进行调用，包含且不仅限于用户服务、接入服务、业务服务、引擎服务、基础服务。

提供业务的分发处理、协议解析、日志管理、并行计算等。

支持集群部署，硬件服务器的伸缩扩展，硬件资源分配服务节点。

支持各功能模块无缝平滑升级。

提供引擎管理服务，支持各类语音服务的在线体验。提供引擎能力 SDK 的下载；支持 API 网关接入的应用管理，对应用访问 API 服务时需要有安全秘钥。

**2. 引擎管理服务**

提供各类语音服务的在线体验，用户可上传音频、文字进行处理。

支持 API 网关接入的应用管理，对应用访问 API 服务时需要有安全秘钥。

支持引擎 API 发布到相应环境多环境，如：线上、预发、测试。

支持创建应用：用于对接入方进行管理，生成接入方接入所需要的接入参数。

支持授权应用：建立接入方和注册 API 之间的关联关系，控制访问权限。

提供系统运营分析及展示、系统日志管理。

**3. 语种识别服务**

提供对给定的一段语音信号分析处理，识别其所属语音种类。支持中、英、维语种的识别，日语、韩语、意大利、法国、西班牙、俄国。

语种识别准确率需大于等于 95%。

**4. 在线听写服务**

提供移动端实时说话的中文、英语、维语、日语、韩语、意大利语、法语、西班牙语、俄语转文字功能。

提供离线文件的转写服务。

在线听写服务要求对于日常使用的常用对话（包含短信类、生活、交通、娱乐、科技、数字数值、名人、互联网热词、新闻等领域）的识别准确率大于等于 95%。

支持端点检测，通过对输入的音频流进行分析，确定用户说话的起始和终止的处理过程。

支持噪音抑制，系统需具备高效的噪音抑制能力，以提高用户在移动办公环境中识

别效果。

提供文本数字规整、文本顺滑等功能；支持中文标点智能预测。系统支持对识别结果语句智能预测其对话语境，提供智能断句和标点符号的预测。

支持热词识别，应用和用户自定义热词集，并在识别结果中给出是否为自定义热词的信息。识别结果应优先从热词集中选取。

移动警务场景下，标准普通话语音识别准确率需大于等于 95%；标准维语语音识别准确率需大于等于 75%；标准英文语音识别准确率需大于等于 85%。

普通话在线听写提供不低于 135 路并发。维语在线听写提供不低于 45 路并发，英语在线听写提供不低于 100 路并发。

**5. 语音合成服务**

提供中文、英语、维语、日语、韩语、意大利语、法语、西班牙语、俄语语音合成。

提供中文语音合成服务，用于在业务应用中实现语音播报、信息提醒、远程呼叫等。并且能够应用新一代文语转化技术，采用最先进的中文文本、韵律分析算法和大语料库的合成方法，合成语音已经接近真人的自然效果。

在移动端场景下，提供多发音人的功能，发音人涵盖男女播音员标准发音、童声发音、机器发音、动漫人物发音、中老年发音、明星发音等。

支持用户自定义分词、读音，可按照用户指定的合成文本分词方式进行语音合成，可按照用户指定的读音或方式进行语音合成。

支持高精度文本分析技术，保证对文本中未登录词（如地名）、多音字、特殊符号（如标点、数字）、韵律短语等智能分析和处理。

支持多字符集，支持输入 GB2312、GBK、Big5、Unicode 和 UTF-8 等多种字符集，普通文本和带有 CSSML 标注等多种格式的文本信息。

支持支持语速、音量、音调等多种合成参数调节。

中文语音合成自然度需大于等于 4.2 分；维语语音合成自然度需大于等于 4 分；英文语音合成自然度需大于等于 4.2 分。

中文合成提供不低于 100 路并发，维语合成提供不低于 45 路并发，英文合成提供不低于 45 路并发。

**6. 机器翻译引擎服务**

实现中文与英文的双向互译、汉语与维语的双向互译。

实现中文与日语的双向互译、中文与韩语的双向互译、中文与意大利语的双向互译、

中文与法语的双向互译、中文与西班牙语的双向互译、中文与俄语的双向互译。

支持对热词/偏僻词进行替换，提升翻译效果。

中英文互译 MOS 评分需大于等于 4.6 分；中维文互译 MOS 评分需大于等于 4.2 分。

支持对于常用且翻译不准确的句子可以添加替换功能,提高翻译效果。

中英互译提供不低于 100 路并发，汉维互译提供提供不低于 45 路并发。

中日、中韩、中意、中法、中西、中俄互译各提供不低于 8 路并发。

**7. 语义理解引擎服务**

支持对自然语言解析，能够给出对应的指令集合。

提供电话、短信、提醒、翻译、查人、查车、查法律、查通讯录等基础语义业务。

为用户提供使用语音发起的搜索功能。搜索的数据范围可根据移动警务业务需要，持续不断的接入应用系统数据源。

提供移动警务业务语意解析字典，包括句式拓展、语义拓展句等内容。

**8. 实时语音转写引擎**

中文实时语音转写实时输入音频流，将音频流数据实时转换成文字流数据结果。将实时语音转换成文字的在线模式。为了使转换后的文本更易读和理解，提供文本数字规整、加标点、文本顺滑等功能。具体如下：

- 支持将中文语音流实时转写为中文文字。
- 说话人分离：支持左右双声道实时语音流转写实现说话人角色分离。
- 智能分句：对转写文本按语义进行子句划分，并在子句之间加注标点。
- 文本顺滑：主要将识别结果文本中将一些不合理的语气词替换。
- 智能标点：根据识别结果给文本内容加上标点符号。
- 多语言混说：支持中英混说。
- 支持 1000 路并发。

**9. 中文非实时语音转写**

非实时语音识别引擎将预先录制完毕的完整音频文件传输至云端，转写服务处理完成后将输出此音频对应的完整文字结果。

语音转文本识别对语音依次进行语音检出、说话人分离、解码等处理。主要功能如下：

- 支持将中文语音文件转写为文字；
- 多种格式支持：支持 8k16bit 或 16k16bit pcm ，支持带语音头的 mp3、wav、

wma、 m4a 语音格式转码；

- 大语音支持：支持大语音文件进行转写(支持 10h)；
- 说话人分离：支持说话人角色分离（两人）。
- 智能分句：对转写文本按语义进行子句划分，并在子句之间加注标点。
- 文本顺滑：主要将识别结果文本中将一些不合理的语气词替换。
- 智能标点：根据识别结果给文本内容加上标点符号。
- 支持 50 路并发。

#### 2.3.6.3.3 数据中台服务需求

**1. 数据业务服务**

实现对移动警务数据针对性数据资源集成，促进数据安全有序的流动应用，完成数据资产盘点与分类分级，有效的对数据资产梳理、完成分类分级，针对不同类型和级别的移动警务数据，部署不同粒度、不同层次的分级分类应用措施，辅助数据应用高效建设落地。

在国家、行业标准基础上，综合系统业务情况和数据特征，制定数据分类和数据分级标准，确定数据分级分类策略。在数据分类策略制定中，根据数据性质、重要程度、管理需求、使用需求等进行数据分类，形成基础信息、人员信息、终端信息、组织信息、业务信息、系统信息六大类别。

在数据定级策略制定中，根据移动警务数据影响对象、影响范围、影响程度等，并结合数据体量、数据聚合、数据实效性等进行综合分析，完成数据定级，确保既达到差异化保护的目的，又不影响具体业务和数据应用。

提供自然语言处理、统计模型、特征分析、机器学习等技术，对采集到的海量数据进行实时或离线分析，可自动并快速识别发现数据，根据分类分级策略智能化处理分类分级标签，可视化呈现数据分类分级结果，发现终端、用户和应用异常行为，并提交系统管理员进行分析研判，及时发现未知的用户、应用和终端的违规行为。

需自主对接现有市局人车卡口数据，视频图像信息库数据，案事件信息，违法犯罪人员信息，机动车登记信息，重点人员信息，勤务信息，互联网舆情数据，车载定位数据，“一标三实”核录数据等公安数据资源，并对外提供应用统一查询接口，为移动警务应用提供数据及服务支撑，在满足移动警务数据传输安全性要求的基础上，支持点对点接口的授权认证、数据的二次加密等安全手段。

提供满足业务需求和技术要求的分布式实时流处理服务，提供服务于流式数据分析、

统计、处理的一站式开发工具，构建一站式高性能实时数据处理框架，依托底层先进的分布式增量计算框架，延迟优化到秒级以上，单个作业吞吐量高达百万级别。

考虑系统建设完成后未来业务扩展，结合各项业务功能使用过程，按照 50000 人同时在线，10 并发的请求，实现最优体验，各类业务平均响应时间要求的需满足以下要求：

- 在网络稳定的环境下，系统最大响应时间小于 3 秒。
- 内容提交操作响应时间平均小于 0.3 秒。
- 普通查询操作响应时间平均小于 0.5 秒。
- 事务处理的响应时间平均小于 0.5 秒。
- 统计分析类查询平均小于 2.5 秒。
- 对外交互接口的响应时间平均不超过 1.5 秒。

**2. 统一用户服务**

提供面向所有服务的用户基础服务，支持对数据可视范围、数据可视字段等权限的定义，针对不同应用提供不同访问权限的服务，平台所有服务的用户基础信息与用户管理服务的数据同步实时变更。

支持与所有的基础设施系统同步（包括运营商 AAA 设备的用户信息以及 PKI 的管理服务用户信息的实时同步）。

与公安内网警力资源库对接，实现基础用户信息的实时同步。

与资源管理服务对接，提供面向第三方的数据实时共享服务，支持对数据可视范围、数据可视字段等权限的定义，针对不同应用提供不同访问权限的服务，平台所有服务的用户基础信息与用户管理服务的数据同步实时变更。

提供用户信息向所有的基础设施系统同步（包括运营商 AAA 设备的用户信息以及 PKI 的管理系统用户信息的实时同步）。

与公安内网警力资源库对接，实现基础用户信息的实时同步。

支持对外提供多种形式的数据同步服务，包括且不仅限于接口、数据库同步。

用户管理服务需与 AAA 认证设备对接，实现与运营商前端设备的用户相关信息的同步。

与证书管理系统对接，实现证书管理系统的用户信息与用户管理系统用户数据之间的实时同步。

支持现有数据的接入以及对外服务的无缝衔接。

统一用户管理作为集中管控服务的一部分，主要提供面向全网移动警务服务和应用

的用户基础、组织机构基础和相关管理服务能力，促进组织机构和用户信息的及时同步共享服务，提高内部信息准确性，降低维护成本。作为整体移动警务平台数据服务的基础，其数据来源于统一的数据资源开发服务中，以数据资源开发服务采集的数据为基础，同时本业务服务能力所产生的数据变化，基于数据资源开发服务的标准进行统一的反馈。具体的业务服务能力如下：

- 提供组织机构和用户基本字段和灵活的扩展字段的自定义延伸。
- 提供多级管理员能力，向下逐级管理、向上严格审批，有效降低内部管理难度。
- 为运营商的开卡流程的流转、审批提供支撑，为各业务单位的用户管理提供流转、审批的支撑能力。
- 提供全面完整的不少于 3 个月的日志服务，所有操作皆记录在案，做到有迹可循。
- 为运营商的开卡流程的流转、审批提供开发支撑，为各业务单位的用户管理提供流转、审批的业务支撑。

**3. 日志数据服务**

根据公安部移动警务集中管控技术标准，制定行为日志、应用日志、设备日志等一系列日志标注，并提供服务面向第三方支持接入日志数据。主要包括所有具有控制能力的安全边界、MDM、资源管理服务、MAM、PKI 等数据采集能力。

形成集中管控日志专题日志数据库，面向集中管控服务提供统一的数据资源支撑。

实时监控采集业务系统、网络设备、安全防护设备的日志信息和安全态势数据，包括流量、日志、系统、威胁情报、系统等。

与公安部集中管控系统对接，实时上报平台所有资源的基础信息和运行信息。

支持满足海量日志数据的实时收集和处理能力。

**4. 综合定位数据及服务**

汇聚车辆定位、电台定位、执法记录仪等定位数据源，统一汇聚并对外提供定位数据服务，包括且不仅限于实时定位、轨迹数据查询服务，满足基于个人、组织、临时组等多形式的查询，支持相关的服务授权和管理。

提供定位数据的统计能力、展示能力以及对外提供的服务接口能力。

数据采集、上报、实时查询服务并发响应时间不大于 1 秒，历史数据查询服务不大于 5 秒。

**5. 泛物联网终端数据服务**

实时接收泛终端智能协同云服务的设备信息、运行数据，统一汇聚并对外提供泛终端数据服务，包括且不仅限于终端动态拓扑服务、终端历史、实时数据、多终端数据服务等。

**6. 技术指标要求**

提供数据资源开发服务，对来自无线终端、互联网采集、二类三类采集的数据具有存储、分析、处理、使用和同步到公安网。

提供实现数据的接入、存储和处理使用。

支持通过跨网文件和服务调度系统，将数据定期汇总进入公安信息网。

支持对数据库结构化数据、文件数据、消息队列数据、日志数据等不同类型的数据进行数据接入任务配置，并根据不同数据特性设定离线、实时数据引入任务或通过解析数据库日志进行库同步等方式，将分散的数据进行统一汇聚，完成数据的分类整合以及数据特征提取。

支持对采集的数据依据业务元数据、技术元数据及管理元数据三个维度对中台本身的元数据进行管理。

支持对数据标准的管理，可以定义标准、标准映射和数据标准字典管理。

支持对存入数据池的数据定义数据质量标准，并对数据质量进行监测和展示。

支持对存入数据池的数据按模型进行加工，支持对模型的自定义。基于任务组件和转化组件，以图形化的方式，实现数据集成流程的快速编排。

支持将常用能力抽象为典型场景，从业务视角定义事件的相关参数既能够实现用户的业务场景。

支持从项目和流程情况、流程运行情况、基础设施情况、流程执行趋势及项目对比情况等维度，对流程部署和运行情况进行总体统计分析。可从任务排程统计、任务执行统计、任务耗时统计等维度进行任务相关的统计分析，便于进行流程优化。从任务和资源的视角对任务的依赖关系和影响进行分析，进而能够跟踪到任务所操作的库表的血缘和影响分析，能够展示哪些任务在操作哪些表的哪些字段，也能够看到是流程中的那个组件在操作哪个表的哪些字段。

支持数据库服务化，依托数据库生成 REST（或 RESTful）架构数据网络服务。支持通过图形化界面配置生成 API 数据服务，并将服务部署生效。功能包括数据的查询，新增，修改和删除等。同时支持通过编写脚本来实现服务化。支持服务化的调试。

提供统一的 API 网关，实现 API 网关的服务接口管理与调度功能、接口管理功能以

及日志管理功能。支持动态管理和配置，持路径的全量匹配和前缀匹配，提供 http 和 https 协议转换功能，同时可以对 https 证书进行检查。支持流量控制调度、负载均衡调度、服务版本管理、服务故障分析、故障转移、流量转移、服务熔断等能力。

提供数据服务网关能力，支持服务目录编排、服务全生命周期管理、服务授权访问、分类管理、监控告警、统计分析和日志审计能力。

提供数据治理与数据资源设计能力，支持数据深度加工与处理（数据采集抽取、过滤、去重、格式转换、质量校验、要素提取、数据管理）。

支持按照业务需求进行数据资源层主题的设计。

#### 2.3.6.3.4 公共基础服务需求

面向全局应用开发提供共性基础服务的支撑，支持接口级、页面级、开发包级的提供。

所提供的公共基础服务需按照统一的资源接入标准服务与资源管理服务实现对接，由资源管理服务统一管理并面向应用提供远程服务。客户端服务组件集成到移动服务总线，服务端服务组件集成到服务总线。

客户端服务组件取消对终端的调取模块，保留业务处理能力，作为独立 SDK 包集成到移动服务总线中并提供相应的服务。

基础服务统一封装对外提供调用，支持 H5、API 形式的应用调用。

**1. 泛终端业务管理系统**

泛终端业务管理系统是按照北京市公安局相关要求，以实战为目标，以增效减负为设计原则，建设的多形态移动警务终端管控系统，实现对 5G 执法记录仪及智能终端的统一管控与应用。

泛终端业务管理系统以泛终端协同服务能力为底座，从泛终端协同服务平台获取设备的注册信息、流媒体信息、设备控制能力等多维度服务能力。以此为基础构建业务管理系统。

系统主要提供设备一张图、视频监控、抓拍管理、数据管理、告警管理、设备管理及系统管理等功能，主要实现终端设备的集中化、可视化管理，人脸图像比对、抓拍告警，执法资料证据（音频、视频、图片）管理等功能。

**2. 跨网安全文件服务**

结合移动警务规范网络边界安全规定的要求，通过与边界互联，实现文件和接口服务的跨网调度。

最大支持文件大小不小于 500M 的单文件的传递，支持并发不低于 500 次/秒，支持断点续传能力，根据硬件设备的供应情况可自主调整并发传递文件数量。

支持包括但不仅限于视频、文本、图片、压缩文件等不同文件格式。

提供根据文件名、时间、应用名等不同维度的日志检索服务。

与资源管理服务对接，提供文件跨网服务。

与集中管控服务对接，按照应用日志接入标准要求提供文件传递的实时日志信息。

**3. 二维码服务**

提供二维码相关服务，实现全市移动警务二维码统一制码、统一扫码、二维码链接数据的互联互通业务目标。

提供独立的二维码扫描服务，支持主动唤起第三方应用。同时支持被三方应用唤出，支持基于 WebVIEW 的界面展示。

与移动服务总线对接，提供包括但不仅限于二维码加密、解密、二维码生成、二维码更新等接口服务。

提供二维码私有协议加解密调用、存储服务。

提供静态二维码服务，支持文字、图片、颜色编辑、尺寸设置、容错率设置能力。

提供活码数据管表管理、数据维护、展示的服务。

提供动态二维码的创建、定时器、修改、删除能力，并对外提供接口服务。

支持不同维度的二维码使用统计，包括应用、二维码活码、动态二维码、终端应用、用户维度、时间、类型等等。

支持不限应用数量的应用支撑能力，支持同时在线终端数为 11 万，并发要求不得低于 500 次/秒，服务响应时间不得高于 1 秒。

**4. 综合定位服务**

提供支持基于移动警务装备的融合定位服务，基于 GPS、运营商基站、WiFi、北斗差分定位等的融合定位方式。提供终端 LBS 定时采集和实时采集的能力。支持基于累积的 WiFi 及基站地理数据库信息，结合用户实时上传的定位依据信息，提供 WiFi/Cell/GPS/IP/北斗差分混合定位算法。

提供以季度为单位提供定时更新基站、WiFi 基础信息库服务。

提供定位采集频率、上传频率、实时采集频率的设置管理能力。

提供定位信息的全文检索服务。基于内网地图的展示服务。

提供移动地址匹配服务，提供北京地名地址库、提供自定义地址维护服务、正向反

向地址匹配服务。

提供 LBS 保活服务。

支持室内定位，定位精准度偏差不得超过 20 米，室外不得超过 10 米。

提供 7×24 小时不间断差分数据推送服务，可用率保障 99.9%。

提供不低于 60000 个高精定位服务授权。

基于虚拟参考站技术推送差分服务，可根据客户要求动态调整推送服务覆盖范围。

与移动服务总线集中服务对接，开放所有的客户端调用接口。

应用层面支持面向所有第三方应用开放数据服务，支持终端数量不得低于 11 万，同时在线终端数不得低于 11 万、并发不得低于 1000 次/秒。

**5. 北斗授时服务**

网络接口：配置≥6 个 10/100/1000M 自适应以太网接口（电口），支持 NTP/SNTP 协议。支持 MD5 安全加密及证书加密协议。

支持单北斗接收机及铷原子钟（驯服守时）。

授时精度：NTP 同步精度优于 2 毫秒（典型值）。

守时能力：在卫星信号丢失情况下，利用内置铷钟应能保持长时间高精度授时。

提供 TOD、10MHz 频率、1PPS 秒脉冲等多种输出接口。

抗干扰：具备抗干扰识别算法，能够识别并隔离欺骗式干扰信号。

管理与维护：支持 USB 端口进行系统升级及日志下载；具备干接点告警功能，提供配套的全网时间统一监控软件，支持对全网终端及服务器的时间同步状态进行可视化监控和管理。

支持双机热备冗余架构设计，支持双设备之间可实现自动切换，确保单点故障时授时服务不中断。

**6. NFC 服务**

提供基于终端 NFC 芯片的读取能力服务，通过终端使用 NFC 的方式读取身份证信息，并与公安内网的身份证解码服务器实现对二代证身份证信息的联网读取。

与移动服务总线对接，实现服务接口的开放。

NFC 客户端需支持多类型操作系统的终端，如：安卓、鸿蒙等

与集中管控服务对接，实现服务日志数据的实时上报。

支持不限数量的应用的使用，支持不低于 200 路并发，并随着业务的发展动态拓展，确保服务资源使用率不超过 60%。

**7. 统一认证**

为各应用提供基于数字证书凭证的认证接口来实现统一认证服务。

支持不低于 1000 次/秒的访问并发，并随着业务的发展不断拓展。

集成 CA 颁发的证书链，通过证书链和 PKI 提供的证书状态查询、吊销列表等基础能力实现对用户的统一身份认证。

与泛终端物联协同服务客户端服务集成，为所有警务应用提供统一身份认证。警务应用通过门户提供的接口获取用户证书并发给应用服务器完成身份认证。

与集中管控服务对接，按照应用日志的标准规范实时上报服务数据。

支持基于用户身份证书的认证、终端设备证书的认证、通讯证书的认证。

与集中管控中心对接，实现向集中管控中心实时上报日志数据。

**8. 统一授权**

提供部署在联网服务子平台和公安信息网服务子平台中的统一认证授权服务。

支持不低于 1000 次/秒的访问并发，并随着业务的发展不断拓展。

提供“应用”级粒度进行授权控制，即授权某用户是否可以访问某个应用。

提供给应用统一用户信息接口，各应用通过获取用户信息 ID 实现对用户的应用级权限管理。

提供对资源管理服务的授权，授权系统也是将其看着一个应用，即控制某应用是否可以访问使用资源服务。具体某个用户可以访问移动信息资源服务子系统中的哪些资源类目，由移动信息资源服务子系统负责权限控制。

**9. 视频会议**

视频会议基础用户数据和组织结构数据需基于统一的数据资源开发服务，包括组织机构、用户信息和组信息。

提供面向二类区、三类区用户的使用需求，支持二类区和三类区的视频会议同步。视频的跨网需基于统一资源管理服务进行，视频协议满足资源服务的跨网视频协议要求。

提供固定会议室能力，支持对固定会议室的集中控制。

基于融合通信服务能力，支持基于即时消息、短信等形式的会议邀请形式。

视频服务需满足融合通信服务对视频流格式的要求，优先考虑国产视频会议服务。

具有会议管理、会议录制管理、第三方服务管理、视频通讯 APP 的能力。

提供点对点、临时视频会议组的视频会议能力。

支持对会议的控制能力，包括且不仅限于会议参会人员的管理、会议现场的管理、

会议的录制、其他人静音等功能。支持统一的集中会议控制模式和单会场的会议控制模式。

支持不同网络质量下的视频会议的质量控制，支持以流畅为前提的分辨率的自动调整等能力。要求网络丢包率小于 20%时可以保证视音频流畅度。

不少于 450 方同时入会情况下，视频会议视频编解码处理延迟小于 30 毫秒 。网络正常的情况下，视频会议整体延迟小于 300ms。

支持包括但不仅限于 SIP、HTML5，WebRTC 等标准协议。

支持包括但不仅限于 1080P、720P 等多种视频处理能力。

支持 5 组高清多点交互式高清会议同时录制。

满足近三年视频 11 万终端入会的会议使用需求，且可通过调配云端池化计算资源平滑扩容支撑能力。

按照融合通信服务的视频流服务要求，提供视频会议的相关服务，支撑第三方的应用进行调用，包括且不仅限于：视频会议的发起、视频会议的挂断、视频会议的控制、会议人员的管理等等。

为各交通支大队提供专用语音网关设备（支持 SIP/模拟中继接入），安全汇接本地运营商中继线路，实现对外热线电话的物理隔离接入和语音的汇聚分析。

**10. 即时消息**

提供 SDK 形式和 API 形式给第三方应用，支持第三方应用建立即时消息的应用。

提供建群、群管理、组聊、单聊等基础即时消息功能。

提供自定义标签能力，支持第三方应用转发消息体到即时消息系统内。

支持第三方应用通过进程间通信模式（IPC），打开即时消息应用使用消息收发功能。

**11. 统一登陆**

提供多类型终端上不同形式的统一登录服务。

在单人单机上，提供基于身份证书的统一登录能力。

在多人单机设备上，提供基于基础库的用户信息统一登录能力。

在非实名认证使用设备上，提供基于设备信息的统一登录能力。

**12. 大模型服务平台**

为支撑智能体和人工智能助手的意图识别的核心推理与决策能力，平台需具备以下大模型服务：

- 多模型调度服务：支持接入并灵活调度多种主流多模态大语言模型，实现负载均衡与择优调用。
- 提示词工程与优化服务：提供系统角色设定、思维链模板及提示词自动优化功能，以稳定并提升智能体的输出质量与可靠性。
- 安全与合规审查服务：集成内容安全过滤器，对智能体的输入和输出进行实时审查，确保内容符合法律法规与道德标准。
- 提供公安业务场景持续运营优化服务，定期对知识问答准确率、业务匹配度、内容合规性进行监测与迭代优化，确保模型输出符合公安业务规范与执法要求。
- 定期对内容进行常态化增补、校对与向量库重构、文档分块、索引优化、检索增强（RAG），知识库更新、增量同步。
- 提供模型运行效果运营分析服务，定期形成运营报告，包括调用量、响应时延、异常对话、误判案例等分析，并针对性开展数据清洗、标注、结构化处理，问答语料构建、意图识别优化，对话日志分析、bad case 修复。
- 提供内容安全与合规运营服务，对模型输入输出进行全量安全审计，及时发现并处置涉敏、违规、误导性内容，建立敏感信息拦截规则动态更新机制，确保符合公安数据安全与保密管理要求。
- 提供用户行为与业务场景运营支撑服务，结合基层实战使用反馈，优化交互流程、功能入口与问答逻辑，提升民警使用体验与业务办理效率，支撑智慧警务、便民服务等场景长效落地。

**13. 无线核录服务**

对接公安网核录系统，封装核录服务，为无线核录业务提供公共服务，实现服务互备提供高可用的核录服务接口。

提供核录轨迹上传管理，监测管理实时回流与定时推送服务。

支持缓存核录记录，缓存核查轨迹，并且抽取公安网核录系统非移动端轨迹信息，用于无感核查比对服务。

构建核查比对底库，建立核录警示信息、自定义警示信息、核查轨迹的缓存库，支撑查询比对服务。

支持核查信息接收，实现核查信息接收功能，接收待比对的人像信息对应的身份信息，列表展示参与核查的人员信息清单，提供页面查询展示功能。

提供核查比对服务，基于核查比对库，实现无感核查比对服务功能，获取待比对人

员信息，提交进行核查比对。

核查比对结果推送，实现比中结果自动推送、结果推送配置管理、比中结果推送监测。

提供核查比对统计分析，实现对核查比对的多维度统计分析。

核查比对服务监测，实现核查比对服务情况的实时监测和统计分析。

提供智能布控管理能力，包括任务的录入、查询、修改、撤控、续控、规则管理等。支持进行精确的布控任务执行与监控。

对接数据中台日志审计系统，实现核录消息日志管理，记录自动比对任务执行情况，结果推送情况，以及记录系统操作日志，实现日志查询管理。

支持与公安网核录系统实现用户管理、基本信息、警示信息、接口服务等内容，支持统计分析等多方面实现授权到民警层面，并且实现可配置化授权。

提供异常行为监测能力，及时发现不健康的应用服务接口，异常的流量信息以及非法 IP，记录用户行为实时判断是否存在越权访问等，实现事前就阻止非法行为发生。

#### 2.3.6.4 应用开发过程管理服务需求

##### 2.3.6.4.1 应用管理服务需求

移动警务应用管理服务是移动警务平台统一的应用管理和分发中心，在新任务书和技术规范的要求上，需新增对网关、扩展类终端上运行的应用和服务进行统一管理，需提供支持不同系统环境下的业务应用的生命周期管理能力，同时满足对移动警务智能终端的上业务应用的管理、边缘网关、扩展类终端上业务应用的管理和分发能力。

借助移动终端管控服务能力，面向不同终端分发不同的业务应用。

基于边、端资产接入和管理能力实现对业务部署的分级展示，实现云-边-端业务部署的一体化展示。

根据边、端安全管控的技术标准，提供对网关、直连终端、扩展终端上的业务服务部署情况的分级监测与上报。

支持提供配置，实现上报数据在云端、网关端的二级缓存和上报，支持根据配置实现边、端信息的层级上报和直连上报模式。

服务期内提供适配终端应用服务，终端类型包括且不仅限于安卓智能终端、嵌入式系统终端、linux 智能终端等。

支持原生应用、元服务、轻应用卡片等不同应用形态的管理。

提供与公安部移动警务平台应用管理服务平台的对接，实现应用数据、应用行为数

据的实时上报。

提供应用远程管理的相关服务接口给第三方服务调用，应用远程管理的服务接口包括且不仅限于：应用的远程分发、远程卸载、应用信息的远程获取、应用的服务数据接口等。

其他终端的应用根据不同的网关类型和终端类型、业务形态制定不同的管理和对接方法，作为预置到智能终端的业务监测的需求，具体如下：

- 提供针对移动警务应用的统一管理和分发操作服务，统一进行应用的管理，并针对三网进行发布和远程管控。
- 提供针对基于 HTML5 研发的轻应用和原生安卓应用的远程管理，包括远程分发、卸载、更新，支持基于统一用户管理服务中的组织、临时分组、个人进行远程管理操作。
- 提供对现有终端已发应用的无缝过渡能力，确保已有终端应用不受影响。
- 提供应用标签自定义的服务，满足不同的分类需求，标签类型在满足公安部移动警务标签类型的基础上，支持自定义的扩展。
- 提供应用版本管理、维护、排序、打分、点评、汇总计算等能力。
- 提供应用的下载、更新管理。提供应用的分发下载以及应用的手动下载两种下载模式服务，提供应用版本增量更新(节流更新)和全量更新能力，支持下载以及更新的断点续传的能力。
- 支持不低于 11 万终端的应用分发。
- 支持基于用户管理服务中组织机构下的多级管理，各级管理员可以查看本机构（不能查看同级不同机构的）、上级、下级发布的应用，只能编辑本级应用，可以分发上下级应用。
- 提供包括公安信息网内、移动信息网内和移动互联网内的应用发布与管理，支持对三种不同类型的应用统一后台管理。支持跨网级联服务，提供基于协议转换跨网的服务提供能力。
- 提供应用的下架审批，以及对历史已分发应用的批量回滚操作。
- 提供应用的黑白名单管理，根据应用安全管控的要求对黑白名单应用进行远程监控和操作。
- 提供包括不仅限于按时间范围、区域、机构、警种等维度统计分析应用的下载、安装、综合评分、升级等指标以及可统计分析应用的增长趋势、访问量趋势。

#### 2.3.6.4.2 开发者支撑服务需求

##### 2.3.6.4.2.1 应用开发过程管理

**1. 社区服务**

提供应用开发者注册审批、应用注册审批、应用密钥申请审批、平台公共资源的申请审批、应用上架审批的全流程管理服务。

支持邮箱、终端号注册。

提供公共服务资源的信息维护和展示，提供模板下载，资源申请和审批服务。

提供应用上架到应用市场服务，实现对生产应用和测试应用的不同环境的上架模式。

提供开发者交流论坛服务，满足开发者日常技术交流、提供相关开发文档上传、信息资源共享及日常工作事项办理的综合管理。

**2. 项目管理**

提供项目过程管理、代码管理、测试管理等全流程服务，支持日常开发管理，包含迭代、任务、缺陷、测试、代码的管理以及持续集成的服务支撑。

##### 2.3.6.4.2.2 资源的管理和发布服务

提供资源的管理和发布服务，为平台的开发资源实现统一的管理和发布，提供对应的资源申请表供用户下载和上传。

与资源管理服务、应用管理服务对接，实现开发资源、应用的自动化配置能力。

**1. 移动警务标准化体系服务**

需提供移动警务标准化体系服务，用于移动警务的管理、指导、应用、开发、发布的标准体系建设，服务需具备：

- 能够进行文件上传，文件审批。
- 能够进行文件预览，文件发布。
- 能够进行文件版本管理，在线编辑。
- 能够进行文件权限管理，包括只读、可编辑、下载等。

#### 2.3.6.4.3 智能体应用开发支撑服务需求

##### 2.3.6.4.3.1 提供智能应用开发支撑服务

提供智能应用开发支撑服务能力。

支持快速生成原生应用和 HTML5 轻应用。

支持通过 UI 控件组装的形式自动生成业务应用，支持对控件的参数进行设置。

支持通过第三方的接口协议自动生成前端 UI 控件。

支持自定义工作流引擎，支持业务自定义流转。

支持根据前端表单自动生成数据库服务。

支持整合平台提供的基础服务资源和数据资源、服务资源的能力，通过可视化控件自由组合的方式，支撑快速生成移动应用，减少移动应用建设对技术能力的依赖。

支持集成第三方 SDK 开发包，面向 H5 应用提供服务。

支持生成的应用直接通过统一的上架审核进入应用市场。

要求智能应用开发服务所使用的用户信息来源于统一的用户服务。

支持第三方能力服务的对接和使用。

服务期内提供咨询支撑服务。

与统一用户服务对接，实现用户信息的共享和权限管理。

与开发者支撑服务对接，实现应用上下架的流程化管理。

与资源管理服务对接，实现对第三方能力服务的配置和调用。

#### 2.3.6.4.3.2 提供 AI 智能体应用开发支撑服务

结合 AI 和大模型能力实现智能体工作流的快速开发和配置服务能力。

**1. 核心能力需求**

支持快速生成对话式智能体与具备规划、执行能力的自主智能体。

支持通过技能插件组装的形式构建复杂智能体应用，支持对插件的参数与触发条件进行灵活配置。

支持通过接入外部工具与 API，自动封装并扩展智能体的行动能力。

支持自定义智能体工作流与记忆机制，支持复杂任务的分解、执行与状态持久化。

**2. 插件服务需求**

为实现智能体的多样化能力，平台需集成或开发以下核心插件服务：

工具调用插件：提供标准化的工具调用接口，支持智能体执行如信息查询、数据计算、内容生成等具体操作。

知识库检索插件：为智能体接入私有或公共知识库，支持基于向量的语义检索，增强其信息准确性与专业性。

长短期记忆管理插件：提供会话记忆、用户偏好、历史交互等信息的存储与读取服务，实现智能体的个性化与连续性对话。

**3. 多模态 AI 服务需求**

为实现智能体与用户更自然、更无缝的交互，并拓展其应用场景，平台需集成以下

多模态 AI 服务：

自动语音识别服务：提供高准确率、低延迟的 ASR 能力，将用户的语音输入实时转换为文本，支持智能体在语音交互场景下的理解与响应。

文本到语音服务：提供自然、流畅、富有表现力的 TTS 能力，将智能体的文本回复转换为逼真的语音输出，增强交互体验与可访问性。

机器翻译服务：提供快速、准确的实时翻译能力，支持智能体在跨语言对话、内容本地化等场景下打破语言障碍，服务全球用户。

多模态理解与生成服务：支持图像、视频等非文本信息的分析与内容生成，使智能体具备“看图说话”、图文报告生成等更高级的认知与创造能力。

**4. AI 助手服务需求**

在终端上提供系统级终端助手，用于对民警语义意图进行理解，识别，分发后调用前后端工具及智能体，实现民警任务处理，提升民警工作效率。

提供终端助手智能输入输出能力：支持长按电源键唤醒助手；支持文字，语音，图片方式的内容输入；输出内容支持语音播报、复制、二次编辑、附件展示。

提供终端助手意图识别能力:支持对外提供意图框架公共服务,实现与移动警务 APP 的对接；支持通过终端助手统一入口进行意图自动分发机制，系统可根据用户语音指令及识别出的业务意图，自动路由至对应已对接的智能体，实现智能化调度与执行；支持基于通用 Skills 机制的意图理解和任务分发。

提供终端助手对话管理能力：支持对话引导和追问问题；支持当前会话或任务执行过程的用户短期记忆和上下文理解；支持跨会话的用户长期记忆，用于实现个性化、用户偏好、历史交互。

提供终端助手与第三方系统对接和业务场景能力：支持对第三方智能体的统一接入和管理，包括但不仅限于上架、下架和分发管理，支持对接的智能体进行标签分类管理；提供帮写帮填能力，提供终端操控能力（包括相机、录音机和通话）；提供在工作区内移动警务 APP 根据用户使用的频率智能推荐能力；支持通过 OpenAI 和自定义接口形式对接三方智能体。

提供终端助手运维服务：支持对业务智能体进行日活/平均使用时长统计；支持对问答内容进行评价，形式包括但不仅限于点踩和主动反馈。

### 2.3.7 业务应用使用服务需求

结合用户对象、业务场景、数据资源共享来源等因素，将移动警务应用进行分类管

理。

### 1. 应用系统部署要求

Ⅰ、Ⅱ、Ⅲ类移动应用系统部署如下图所示。


**应用系统部署示意图**

### 2. 应用标准要求

（1）用户授权访问控制。应对用户进行基于角色的授权和访问控制。用户的信息访问授权应遵循“最小权限原则”；管理角色授权遵循“特权分散原则”。

（2）系统权限访问控制。应按照“最小权限原则”限定终端系统权限访问，不得申请开放本应用不需要的终端系统权限（如启用 GPS、打开摄像头、读取通讯录等）。

（3）日志管理与安全审计。应按照统一要求，对用户登录/退出、关键数据操作等行为记录日志。应用日志必须保留用户身份信息，满足历史信息可倒查要求，并按照规范提交集中管控中心。

（4）应用数据加密存储。移动终端应按照规范对重要数据进行加密存储。

（5）资源访问接口要求。应遵循资源提供方的技术接口及管理规范。

（6）支持安卓操作系统、鸿蒙操作系统等操作系统。

此外，平台提供移动警务应用服务，包括工具类服务和 SAAS 应用服务。所有应用服务都需按照移动应用开发标准接入，并与集中管控系统对接，实现应用行为的实时上报。应用中使用的用户信息，都需与用户管理服务进行对接，实现用户信息的统一调度。

#### 2.3.7.1 移动警务应用服务需求

所有应用服务都需按照统一的开发和接入标准进行提供，包含且不仅限于以下内容：

统一使用日志存储服务。

大文件的数据的跨网同步，必须通过文件摆渡的服务，不能使用接口服务形式。

所有应用都必须对接集中管控服务，按照应用日志的对接标准实现业务应用的日志实时上报。

所有应用都必须实现基于 PKI 的身份、应用的签名和使用时的签名认证服务。

所有应用都必须与门户完成对接，实现应用的单点登录能力。

应用的用户信息都必须与基础用户服务对接，根据基础用户服务提供的权限使用用户信息。

服务中所需要的基础服务组件，都必须使用统一提供的服务组件以及基础能力，包括统一推送、统一认证、语音识别、NFC 等服务。

Ⅰ类应用必须进行基本的本人本机本应用认证方可使用，需进行终端号码+终端串码和应用的注册。

应用服务期内，根据用户需求实时调整。

**1. 邮箱服务**

在移动警务终端实现邮箱服务，打通与内网 PC 端邮箱系统的对接，面向全局民警提供实时收发和邮件处理服务。

基于用户服务提供邮件联系人的维护服务，仅支持维护自定义特色字段。

要求实时同步位于内网邮件服务器上的邮件信息，实现 PC 端、终端两端间的邮件信息同步。

提供基于邮件标题、内容的全文模糊检索服务。

提供邮件收取、邮件发送、星标邮件。

备注、邮件删除、同步删除等功能。

提供文件夹自定义功能，提供邮件分类的能力。

支持 6 万终端的使用需求。

**2. 任务助手**

提供警务任务发布与管理服务能力。

支持任务流转过程中自定义任务流转过程和自主选择任务执行者。

支持任务自定义转派，支持自主定义任务执行角色和任务查看角色。

支持任务内容的表单自定义能力。

支持任何警务人员发布主任务、子任务，发布任务类型包含且不仅限于巡逻类、站岗类、勤务类，且可选择任务人员、任务时间、设置任务提醒等。任务发布后，关联人员收到任务提醒，执行人员可以针对任务进行任务完成、任务转交、任务上报等操作。

支持发布人员作为管理者对任务进行重新分配与任务人员临时调度的操作。

支持在任务过程中，发布者与执行者实时进行任务会话、发送图片、发送附件、发送日报等方式进行交流，并保存一切行为记录，做到有痕迹、可追溯。

支持任务人员工作状态全局展示，避免出现一人多任务的问题。

支持任务执行者每人的任务都会在任务发布者手中有实时记录，发布者者通过对每位执行者的任务线的监督，对任务实现全局把控。

支持任务中发布的所有文件统一归档，保存在任务文件中，任务中上报的所有问题，以及聊天内容，在任务结束后自动形成任务记录，生成任务记录链接，通过即使消息和通知推送给任务相关人员，任务相关人员也可通过任务助手的“任务记录”模块，下载相关文档。

支持回溯任务历史，通过任务记录查看出现问题的环节，准确定位。

支持查看个人任务记录，可看到自己接收的、发布的、与自己相关的任务。

支持 6 万终端的使用需求。

**3. 通讯录**

以数据资源开发服务中的组织机构和用户数据为基础，提供通讯录的展示和维护相关服务。

维护数据按照数据资源开发服务的要求，实现实时更新。

提供警务通讯录的详细查询和检索功能。

支持权限范围下的机构信息查询、分组信息查询、通讯录成员信息查询。

支持根据组织机构名称、分组信息名称、通讯录成员信息等所有涵盖的字段进行模糊的匹配查询。

支持第三方应用集成通讯录服务。

支持 6 万终端的使用需求。

**4. 论坛**

提供论坛帖子分类、帖子板块、帖子浏览、发帖、评论、点赞、分享、话题讨论等功能。

提供面向管理者的管理员管理、分类管理、版块管理、帖子审查、话题管理、帖子推荐、帖子置顶、禁言用户、设置敏感词库等功能。

设立版主用户，协助管理员对板块进行维护管理，并提供版块内的帖子审查、话题管理、帖子推荐、帖子置顶、禁言用户等功能。

要求支持文件附件等内容存入对象存储。

支持移动端、PC 端、管理端。

支持不低于 6 万终端使用需求。

**5. 云盘**

提供面向移动端的云盘服务，支持云盘的文件查询、分类存放、存储、删除、分享等操作。

提供自定义的文件夹编辑服务，并对文件进行归类。

支持对用户存储空间的配额编辑，同时，可以基于用户的使用情况，弹性共享所有用户的剩余存储空间。

提供云盘的 Web 管理能力，实现文件的查询、分类、存储、删除等操作。

支持多类型的文件存储，包括图片、视频、文档等类型，支持所有格式文件。

要求支持文件附件等内容存入对象存储。

与资源管理服务对接，支持面向第三方应用提供文件的接口服务，包括不仅限于文件的上传、文件夹的维护、文件的删除、文件的编辑等。

支持不低于 6 万终端的使用需求。

**6. 视频会议**

视频会议基础用户数据和组织结构数据需基于统一的数据资源开发服务，包括组织机构、用户信息和组信息。

提供面向二类区、三类区用户的使用需求，支持二类区和三类区的视频会议同步。视频的跨网需基于统一资源管理服务进行，视频协议满足资源服务的跨网视频协议要求。

提供固定会议室能力，支持对固定会议室的集中控制。

基于融合通信服务能力，支持基于即时消息、短信等形式的会议邀请形式。

视频服务需满足融合通信服务对视频流格式的要求，优先考虑国产视频会议服务。

具有会议管理、会议录制管理、第三方服务管理、视频通讯 APP 的能力。

提供点对点、临时视频会议组的视频会议能力。

支持对会议的控制能力，包括且不仅限于会议参会人员的管理、会议现场的管理、会议的录制、其他人静音等功能。支持统一的集中会议控制模式和单会场的会议控制模式。

支持不同网络质量下的视频会议的质量控制，支持以流畅为前提的分辨率的自动调整等能力。要求网络丢包率小于 20%时可以保证视音频流畅度。

不少于 450 方同时入会情况下，视频会议视频编解码处理延迟小于 30 毫秒 。网络正常的情况下，视频会议整体延迟小于 300ms。

支持包括但不仅限于 SIP 、HTML5，WebRTC 等标准协议。

支持包括但不仅限于 2160P、1080P、720P 等多种视频处理能力。

支持 10 组高清多点交互式高清会议同时录制。

满足并发支持能力不得低于 450 路。

按照融合通信服务的视频流服务要求，提供视频会议的相关服务，支撑第三方的应用进行调用，包括且不仅限于：视频会议的发起、视频会议的挂断、视频会议的控制、会议人员的管理等。

**7. 即时通讯**

支持场景丰富的即时通讯消息功能：除支持文字、图片、音视频、文件等多种即时通讯消息以外，还需要支持回执消息、已读提示等消息类型，以及更丰富的群管理功能。

支持同一用户账号两客户端同时在线（移动端和 PC 端），任意终端接收或者发送的消息，在其他终端上均可以下载漫游记录，包括文件。

支持公安内网 PC 客户端与移动警务专网 APP 和 PC 客户端消息互通。支持内网多版本的终端要求，包括且不仅限于 Windows xp 及以上，安卓 8.0 及以上、鸿蒙等操作系统。

要求支持文件型发送内容存入云上对象存储。

支持对发送的消息、通话录音文件进行审计，查看和下载，以便追溯。

支持敏感词屏蔽功能,依托过滤词典，精准过滤有害信息，屏蔽信息中的敏感词，同时以*方式显示。

支持过滤词典内容自定义添加。

支持消息群发功能。

支持第三方应用通过进程间通信模式（IPC），打开即时消息应用使用消息收发功能。

提供包括但不仅限于按时间段对用户、在线、功能、活跃度进行分析统计，和筛选导出详细数据的能力。

支持公安部移动警务互联互通标准。

支持面向Ⅰ类区、Ⅱ类区、Ⅲ类区用户进行服务，支持并支持三个区域用户信息的同步。

支持多租户模式，支持不同租户之间数据的相互隔离。

与公安部及各省市公安厅即时通讯系统的互联互通，可跨系统建立单聊或群组聊天，实现文本、图片、语音等消息互通能力和文件交换的能力。

对接数据资源开发服务中的用户数据服务，以用户服务提供的用户基础信息作为用户基础，实现用户信息的实时同步，应用侧做出的用户信息修改和日志行为数据，需按照标准纳入数据资源开发服务。

支撑 7 万终端使用服务（支持 6 万民警与预留 1 万机构使用）。

**8. 警讯**

**（1） 应用需求**

警讯应支持以栏目列表形式展现，支持用户对多个栏目进行订阅和取消操作，支持重点栏目和主推栏目通过后台管理系统进行配置，支持配置客户端固定订阅栏目。

栏目内部应支持焦点大图和列表展示方式。警讯内容支持普通警讯、图集、视频、直播等。焦点警讯应支持人工推荐，可循环滑动显示。列表警讯应按综合排序展示缩略图、标题、来源、日期、评论信息，支持添加角标图案等。

警讯详情页应展示标题、正文、图片、来源、评论、点赞等内容，支持通过手势缩放调整字体大小等页面显示效果。支持警讯收藏、评论、点赞、评论回复等操作功能。支持领导在查看警讯进行批示的功能。评论带有敏感词时，系统应进行警告提示，并进行限制发布。

图集类资讯应突出展现图片信息，可全屏显示图片、下载图片，滑动显示下一张图片，最后一页为图集推荐。

直播或视频类警讯，应支持点击视频进行播放，支持暂停、续播和全屏播放。视频

播放过程中进行屏幕拖拽操作时可缩小为小窗口进行播放。

支持警讯专题功能，可针对某个事件内容集中整理收集素材发布成专题，专题支持按照时间轴倒序排列和按版块两种展现方式，支持展现模式一键快捷切换功能。

警讯内容应支持关键词全局搜索，搜索后的结果以列表形式呈现。

要求支持文件型发送内容存入云上对象存储。

**（2） 管理需求**

提供警务资讯 SAAS 服务，提供统一管理的多租户服务能力平台。提供租户账号的注册申请及开户销户等审核管理功能，并根据用户组织机构和等级的不同，分配不同的可用功能范围和使用权限。支持主管理账号创建多个子账号，并分配对应的角色及权限。系统应提供数据统计功能，为用户提供相应的数据统计及报表展示功能。

系统应提供警务资讯编辑、审核、发布，专题制作以及用户评论等全流程业务服务功能。应支持管理员对警讯资讯所归属的栏目进行统一管理，各用户可以对自己所创建的栏目进行单独编辑修改。

系统应提供方便快捷的操作界面，可以对单条资讯进行修改编辑，包含标题、关键字、作者、资讯类型、角标类型以及正文内容及格式等功能。

图片素材上传时，应支持自动和手动裁剪功能；视频素材上传时，应支持自动添加水印功能，同时支持自动抽帧生成多张缩略图，供编辑人员进行选择；视频素材上传后应进行自动转码压缩处理，转码压缩后的视频格式统一为 MP4，码率不应高于 2Mbps。

系统针对实际警务资讯编辑操作的场景，应提供数据清洗和格式转换功能。发稿人员，可以将其它地方的稿件内容粘贴到正文编辑框中，通过数据清洗与格式转换按钮，快速的将原文中携带的无效标识符去除，并按照系统预先设置的标识符进行替换，保障最终呈现效果的统一。

警务资讯的发布严格依照采编及审核发布分离的机制，发稿人在编辑完成后，由审核人员审核确认后，才可以正式发布。审核人员也可以对已经发布的资讯直接进行删除和退为待发布状态。

警务资讯版块应提供用户评论互动功能，管理后台应提供对用户评论的查看和审核管理功能。评论功能可以设置为“先发后审”或者“先审后发”两种工作模式。先发后审模式下，管理员对已发布的评论进行查看，如果发现不符合要求的可以进行修改、删除和临时屏蔽操作；先审后发模式下，用户发布的评论，初始状态下只有自己可见，待管理员审核后，才能被所有人所见。

针对重大警务活动或专项内容，需要以专题形式对用户展示。管理平台应提供专题制作及管理功能。在管理页面中，已有专题以列表形式展示。专题下可以划分为多个内容模块，模块的类型包括：焦点区、五图区、视频、标题列表、图集。用户可根据专题形式，按照自己的思路，自由选取模块，模块数无限制。

资讯管理后台可以对发布的所有警务资讯内容，按照关键字进行全量模糊检索，方便信息管理人员查找历史资料，获取素材。

管理平台中应提供消息推送管理功能。管理员在重要资讯或通知公告下发的时候，可以选择单条资讯进行消息推送，客户端用户即可收到该条推送消息的提醒。

**9. 警圈功能**

**（1） 应用需求**

警圈应支持最新、热门和话题等多栏目页展示形式。

最新警圈应以发布时间倒序列表展现，包含所关注的人员发布的最新警圈及自己的警圈内容；热门警圈内容应根据热门排行以列表形式展现。话题栏目按话题热度进行列表展示。

点击列表中的警圈内容进入到警圈详情页面，展示内容包含发布人头像、单位及部门、发布日期、正文、图片、视频、音频、直播等内容。

警圈版块中应支持@某人和@某个公众号；同时支持通过双#号加关键字的模式，发布为话题警圈。用户对自己发布的警圈内容可以进行修改和删除操作。

各种警圈列表均支持多种类型的警圈内容的混排。图片内容应在列表中默认一行 3 张图片并排显示，点击更多查看全部图片；点击单张图片可以查看大图。

视频内容应支持在列表中直接点击进行小窗口播放；点击全屏按钮后进行全屏播放。列表播放过程中，如果拖拽列表，可以缩小为小窗口继续播放。

长文字内容应支持默认只展示 3 行文字，点击全文按钮后展示全部内容。

各类型内容发布时，应符合以下要求：

- **文字发布**

包含标题、关键字、正文三部分，支持插入话题和自己编辑话题，#话题内容#话题编写形式，也可以选择话题，选定的话题内容会自动插入到标题内容前，以#话题内容#的形式展现，也可以插入图片、视频、音频、地理位置等信息。

标题限制：不得超过 30 个汉字；多个关键词需用分号隔开。

内容限制：不得超过 2000 个汉字。

➢ **图片发布**

可以选择终端里面的图片进行发布，也可以直接拍照发布，图片不超过 9 张，也可以插入文字、视频、音频、地理位置、话题等内容，用户可以选择自动添加水印，同时也可以设置为隐私内容仅自己可见。

➢ **视频发布**

视频内容支持本地视频上传，也可以重新拍摄后进行发布，拍摄时长不超过 90 秒，同时支持插入文字、音频、地理位置、话题等内容，可以设置隐私内容仅自己可见。视频内容上传前，应支持客户端本地转码压缩处理，并支持自动添加水印功能；转码压缩后的视频格式为 MP4，码率不应高于 2Mbps。视频内容上传应支持多线程及断点续传功能，如因本地网络原因受限，可缓存至本地存储，待网络恢复后自动启动后台静默上传。

➢ **音频发布**

可以录制语音进行发布，录音时长不超过 180 秒，也可以插入文字、视频、话题、地理位置等内容，可以设置隐私。

➢ **直播发布**

警圈内容支持视频直播，直播发布时可以设置封面图片、撰写直播主题、可以选择显示地理位置，可以选择直播话题。直播过程中支持前后摄像头切换、画面手势缩放以及麦克风开关操作，观看端的用户评论内容应直接在视频画面上以滚动列表或弹幕的方式叠加显示。直播视频内容应支持与移动警务音视频服务平台进行无缝对接，作为移动警务视频资源进行调取。

针对已经发布的警圈内容，可以进行应用内部的转发，转发过程中可以进行转发内容正文的编辑。对于发布的警圈和话题内容，均支持通过关键字模糊匹配的方式进行搜索；搜索后的内容以列表形式进行排序。默认显示推荐的话题内容。

警圈版块应提供包括用户关注和取消、评论、点赞等互动操作功能。

公众号及联系人信息，均应支持通过关键字模糊匹配的方式进行搜索；搜索后的内容应以列表形式进行排序，已关注联系人及公众号应默认置顶显示。

系统应提供个人设置模块，提供“我的警圈”“我的收藏”“我的评论”“设置”“应用”等个人类操作内容。 同时应提供头像设置、系统设置（消息推送、字体大小调整）、其他设置（意见反馈、关于）、版本更新检测等操作。

**（2） 管理需求**

系统应提供警圈内容的查看和管理，以及用户评论审核等服务功能。平台管理员可

以对下属警员所发布的警圈内容进行查看管理，发现不良信息，可以通过后台直接进行修改，或者对其进行屏蔽操作。

平台应根据警圈内容的阅读量和评论量，按照既定算法选出热点警圈内容排行榜，展示给用户。同时热点内容也可以经由后台管理员进行人工干预，通过人工加权的方式，修改各榜单中的热点内容和排列顺序。

系统还应提供由经过认证审核的公众号账号，通过警圈管理后台进行发布。公众号发布的警圈内容，应在其发布者名称后添加显著标识，以便于用户进行区分。公众号账号只能通过后台管理系统进行登录，不能登录警务客户端；用户在警圈中@公众号，或者对公众号的文章进行评论时，应能在管理后台提醒账号维护者。

警圈内容应提供用户评论及回复等互动功能，管理后台同样应提供对用户评论的查看和审核管理功能。警圈的评论功能为“先发后审”工作模式。由系统通过敏感词过滤等功能对评论进行第一轮审核，审核通过后立即发出。管理员可以在评论管理后台对已发布的评论进行查看，如果发现不符合要求的可以进行修改、删除和临时屏蔽操作。

警圈管理后台可以对发布的所有警圈内容素材，按照素材类型，进行统一编目及分类整理，方便信息管理人员查找获取，以及对素材进行重复利用。

警务资讯管理服务系统应提供用户账号的注册申请及开户销户等审核管理功能。用户需要使用资讯管理服务时，需要在平台提交注册申请，由管理员对其各项基础信息和资质进行审核确认后，为其开通平台使用账号。使用资讯管理服务平台的用户，根据其机构等级、角色的不同，会对应不同的可用功能范围和使用权限。支持一个管理用户在其账号下同时创建多个子账号，并由其主账号为子账号分配对应的角色及权限。

系统应为用户应提供相应的数据统计及报表展示功能，便于用户直观的了解自己的平台使用状况。包括：用户访问量统计，活跃度排行统计，访问时段分布等多种统计报表；警讯发稿量、警讯阅读量排行、热点警讯排行、点赞排行、评论排行等多种统计报表；警圈发布数量、警圈阅读量排行、粉丝数量排行、点赞排行、话题热点排行、分享转发排行等多种统计报表。

### 10. 云输入法

提供语音输入、手写输入、多布局键盘输入三种输入方式。

提供手写输入服务提供自动识别手写输入，并返回相应文字。

提供横屏连写与竖屏叠写两种手写输入方式。

支持输入法联想功能，用户输入拼音后，输入法根据定制的警务词库推荐出候选词。

支持警务词库、个人词库。

支持第三方应用嵌入输入法进行二次开发。

服务期内，需对引擎进行定时的更新（确保至少一年两次），以确保服务的质量。

支持不计应用数量的二次开发服务和支持不低于 6 万终端的服务。

**11. 翻译**

提供汉维、中英、中日、中韩、中意、中西、中法、中俄的实时口语翻译。

提供客户端开发的服务能力，面向第三方应用开发提供服务。

支持对情景例句分级分类展示，用户可播报和收藏情景例句。

支持安卓、鸿蒙操作系统。

查看历史：查询、查看翻译的历史记录。

服务期内按季为单位提供系统更新服务。

支持不计应用数量的二次开发服务和支持 6 万终端的服务。

**12. 智能音视频服务**

**（1） 移动应用服务**

支持固定监控分级展示、点播内容展示、历史视音频分级展示、移动视音频分级展示、第三方平台内容展示及主题分组展示。

支持高（标）清视频及音频实时回传及本地历史视音频文件回传和回传进度展示。支持回传过程中切换、打开关闭摄像头、开/禁音等操作。回传过程中支持浮动窗口、全屏窗口、最小化窗口等多种窗口模式，支持后台静默、邀请及强制回传模式。支持对本地录制的视音频内容进行管理。

支持调取移动警务终端、车载警务终端、固定监控等视频内容的实时和历史数据调取查看功能，支持自动提取视音频流的信息摘要，支持最大同时调取 4 路画面，支持在调取视音频的同时进行本地视频录制。

支持在警员之间以及警员与指挥中心之间发起高清视音频互动，支持邀请和强制互动模式。支持视音频点名。支持将若干设备进行分组并实现分组视音频互动。支持展示当前互动的参与者列表，本端和参与者网络情况，互动持续时间等信息，方便互动参与者了解当前互动状态。

支持对直播和常用固定监控摄像头的标注和收藏功能，支持浏览历史记录的定期同步，支持对警员通知内容的高亮提示和系统通知推送功能。

**13. 融合通信**

基于融合通信服务能力，提供融合通信应用。

提供基于智能终端、PC 端、Web 端的融合通信应用，提供跨网互通的访问能力。

提供包括多种通信系统和方式的通信服务，包括语音、视频、GIS、消息、图传流、语音对讲等。

其中视频服务支持多种形式的视频融合：包括图传流入会、内网非涉密会议入会、移动视频会议入会以及监控入会、语音电话呼叫入会等形式。

提供相关的集中会控能力和点对点的会控能力，会控功能包括且不仅限于：会议视图的设置、会议声音和视频的开关、人员入会、剔除以及会议的加密、加锁等能力。

提供语音对讲的服务，支持 1.4G、800M 的互通呼叫，支持单呼、群呼、强插、强拆、代接、录音、监听等功能。

提供 P-POC 服务，支持 1.4G、800M、350M 的互通呼叫，支持单呼、群呼、强插、强拆、代接、录音、监听等功能。

**14. Web 门户**

提供移动警务二类、三类区的门户网站服务，支持信息的发布、分类、展示、资源的下载。

**15. 互联网即时消息**

提供互联网即时消息 APP 以扫码入队能力，共治力量扫码完成注册、信息填报与人脸识别认证，管理员线上审批即可入队简化人员吸纳流程。

提供组织管理员可维护人员信息、调整组织架构、委派下级管理员能力,支持通讯录按人员类型智能适配展示模式：民警、辅警、文职默认组织架构模式，遵循“上级可看下级、下级不可看上级、跨单位不可见”的数据可视化模式。

支持通过互联网与公安信息网“全国警信”进行合规化文件传输与文件协作能力。

提供完善的即时通信能力，支持单聊、群聊，可发送文字、语音、音视频、附件等多种消息，提供消息撤回、引用、转发、@提醒、群接龙等功能；支持消息分类检索、多维度查找历史记录，配套公众号定向推送通知资讯，适配日常沟通、任务部署、应急通知等全场景协作需求。

支持公安行业数据安全规范，采用最小权限原则，人员权限、信息可见范围、数据流转全流程可管可控；实人认证、权限分级、传输加密等多重保障支撑，确保敏感信息与共治数据安全，适配基层社会治理的安全合规要求。

要求支持安卓系统，鸿蒙 5.0 及以上通过“卓易通”下载，可在主流应用市场下载，

包括且不仅限于华为、荣耀、OPPO、VIVO、小米、应用宝六大应用市场。

### 2.3.8 移动警务安全管控服务需求

根据2016年移动警务总体建设技术方案以及全国公安移动警务升级改造建设任务书要求，以及满足采购人移动警务与视频专网进行有机结合的业务需求，移动警务管理服务包含以下服务要求：

1.提供移动终端的安全管理服务。

2.提供移动终端的应用管理服务。

3.提供边、端的安全接入和管控服务。

4.提供移动互联网服务子平台的应用安全服务。

5.提供移动警务的其他服务需求。

#### 2.3.8.1 PKI密码服务需求

PKI密码服务需符合部标和密评要求。

提供基于国产商用非对称密码算法（SM2）构建移动警务身份认证体系服务，支持产生RSA密钥对、国密密钥对能力，支持双算法四证书。

提供证书客户端，实现统一认证、多因子认证、空中发证服务。

支持鸿蒙、安卓等操作系统。

**1. 证书管理服务**

与用户服务对接，实时获取用户中心维护的用户数据（包括新增、修改、删除），并在此基础上进行证书的制作、变更和注销。

提供基于工作流的证书申请审核流程，要求针对审批执行可查看、可审批、可回退、可转发等操作。

与PKI服务对接，提供证书的注册、补发、更新、延期、下载、查询服务。支持证书信息的冻结、解冻、注销等服务,要求支持批量操作。支持证书密码的修改和加密存储。

对外提供包括且不仅限于证书登录服务，证书认证服务、证书查询服务、证书冻结服务、证书注销服务等。

与公安信息网PKI体系采用同一个根CA和统一格式的数字证书，并实现互认。

提供服务日志的统计和查询和异常服务信息的预警服务，支持对外开放数据服务。

提供密码模块调试以及密码模块初始化能力。

支持SKF接口转JNI接口和设备管理接口开发，支持访问控制接口开发，支持应用

管理接口开发，支持容器管理接口开发，支持密码服务接口开发。

提供应用签名、验签服务，支持安卓附属签名验签能力，并对外提供服务能力。

提供证书管理的客户端，为证书的下发、延期提供用户自主服务。

**2. 证书注册服务**

提供证书申请、审核、更新、注销、挂起、查询和下载等功能。

提供用户信息和证书信息两方面的管理，用户信息的管理可进行灵活的配置。

支持 SM2Key 类型管理功能，可以灵活新增/修改/删除等 SM2Key 设备类型的配置管理；支持 KEY 设备创建应用和指定密钥容器名称。

支持一人多证的签发。

支持批量证书申请，支持新用户批量申请证书。

证书的审核支持自动、手动两种模式。

提供对到期证书更新的功能。

支持证书发放数量和情况统计。

支持查看系统配置的密码设备。

系统支持日志查询、分析、审计功能。

支持自动日志签名。

该系统中的审计业务和其他业务要实现严格的分权管理。

支持 SCEP 协议支持证书注册、获取证书、获取 CRL、获取 CA 证书服务。

支持证书数据导出功能。

支持基于双算法的证书申请、下载、更新、冻结、解冻、注销证书等功能。支持 RSA/SM2 四证一步申请和同步管理功能。

兼容性要求:完全兼容现有的证书数据、用户数据。

**3. 数字证书密钥管理服务**

提供用户密钥的生成、分发、备份、更新、恢复、归档、查询等功能。

提供密钥托管服务，对用户的加密密钥对进行备份和管理，并提供用户密钥的恢复功能。

对进入密钥管理中的有关操作人员及相关操作必须有严格的身份认证和权限控制机制。

系统的运行事件记录、系统重要策略、密钥操作记录、操作人员信息必须有相应的审计机制。

支持查看系统配置的密码设备。

支持自动日志签名。

支持对多个 CA 提供服务，可以通过对各个 CA 系统实施灵活的授权管理实现对各个 CA 系统服务的管理。

系统要求支持方便的司法取证。

KM 要支持预生成密钥功能。

系统中的审计业务和其他业务要实现严格的分权管理。

同时支持 RSA 和 SM2 双算法。

兼容性要求:完全兼容现有的证书数据、用户数据以及密钥数据，可基于现有加密证书密钥私钥数据实现保持密钥更新功能。

**4. 证书目录服务**

支持移动警务证书、CRL 列表发布和查询。

支持与身份认证网关联动，供身份认证网关获取用户的属性证书。

支持主从结构，支持一主多从和多主多从的部署方式。

主从配置时支持自动测试，可以清晰的知道从 LDAP 的存活状态。

支持 LDAP V2、V3 标准。

支持 PKI/PMI 的相关标准，支持 X.509 V3 标准。

可根据某一查询设置特殊的索引进行优化。

能够支持实现基于目录树、基于某个分支的复制。

复制粒度精确到条目。

支持一主多从、多主一从、级联主从、镜像主从等多种复制模式。

具备相应机制保证复制的可靠性。

对无法完成的复制操作，进行重试，并支持多根后缀的复制。

支持订制复制策略，能够指定复制的频度与时间。

支持创建多个目录服务实例。

支持基于“拉”模式的由从目录发起的主从复制。

支持目录数据导入导出。

复制：从目录服务器的宽度超过 100，深度超过 10 级。

最大数据容量：单个目录服务实例可管理亿级条目。

支持多并发处理。最大并发连接数不低于：4096。

支持精确查询，千万级条目下，500 线程精确查询的平均速度可达到 1ms（毫秒）以内。

支持模糊查询，千万级条目下，500 线程混合查询的平均速度在 100ms 以内。

10 万条目吞吐量不低于 2500 次/秒（50 线程精确查询）。

支持在线升级。系统支持在线远程升级。

支持多种复制启动方式：手动启动复制、定期启动复制。

**5. 独立密码机服务**

密钥生成与管理：可以生成 1024/2048/3072/4096 位 RSA 密钥对和 256 位 SM2 密钥对。

密钥的安全存储：设备内可存储 50 对 RSA 密钥对（包括签名密钥对和加密密钥对）和 50 对 SM2 密钥对，并且私钥部分受系统保护密钥的加密保护。

数据加密和解密：支持 SSF33 算法、SM1 算法的 ECB 和 CBC 模式的数据加密和解密运算。

消息鉴别码的产生和验证：支持基于 SSF33 算法、SM1 算法的 MAC 产生及验证。

数据摘要的产生和验证：支持 SM3 杂凑算法。

数字签名的产生和验证：可以根据需要利用内部存储的 RSA/SM2 私钥或外部导入 RSA/SM2 私钥对请求数据进行数字签名。

数字信封功能：支持基于 RSA/SM2 密码算法的数字信封功能，并支持由内部密钥保护到外部密钥保护的数字信封转换功能。

物理随机数的产生：采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的随机数。

用户访问权限控制：具有用户管理功能，提高密码设备自身的安全性。

密钥备份及恢复：支持基于主密钥保护下的密钥的备份和恢复功能，保证安全应用系统的安全性和可靠性。

兼容性要求:完全兼容现有的密码机密钥数据。

提供不低于 3 台独立密码机服务和 2 台云密码机服务。

性能要求：

- 256 位 SM2 密钥对生成：≥350 对/秒。
- 256 位 SM2 签名速度：≥700 次/秒。
- 256 位 SM2 验证速度：≥180 次/秒。

- 256 位 SM2 加密速度：≥130 次/秒。
- 256 位 SM2 解密速度：≥220 次/秒。

**6. 移动身份认证网关服务**

支持移动警务 CA 颁发的数字证书。

支持 RSA 和 SM2 双算法。

支持主路和旁路两种工作模式。

结合警用移动终端数字证书管理系统，可通过扫描二维码方式实现用户身份信息的漫游功能。

支持警员证书等多种证书类型的身份认证，对于公安未来定义的证书类型保持扩展设计，以便在新证书类型出现时能够无缝结合。

支持证书信息传递功能，能够根据不同的公安行业证书结构进行解析，如警员、岗位、机构等证书格式，将基本信息和扩展域信息传递给后台应用。

支持入门级访问控制，能够根据不同的证书类型，对应用的入门级访问进行许可控制，防止岗位和机构等证书对应用的越权使用。

能够根据公安的数字证书格式标准，获取警员的个人、群体、自定义信息。

支持将警员认证信息、属性信息、获取信息发至第三方应用系统。

支持基于用户角色的访问控制。

支持向业务系统传递属性信息。

支持 B/S、C/S 应用系统接入。

支持以 SYSLOG 标准方式发送证书登录日志。

支持 TOP N 功能。

支持双机热备，防止单点故障。

能够对管理员进行限制。管理员通过证书验证后方可获得集中认证网关管理系统的权限。

能够支持系统备份、恢复。

系统支持通过 OCSP 协议方式对证书状态进行验证，更实时、更准确。

系统支持通过证书基本属性、证书扩展属性、用户属性、时间、终端地址、硬件设备特征以及信任域进行业务系统的授权和访问控制，通过不同条件的组合做到灵活授权。

系统支持对后端业务系统负载，在不使用第三方负载均衡设备的情况下实现对业务系统的负载效果。

兼容性要求：支持完全兼容现有应用改造模式，要求现有已完成对接的应用系统，在 APP 以及应用服务端不做任何调整的前提下，完成对接工作。

性能要求：

- 新建连接速度（次/秒）:≥3000；
- 最大并发连接数:≥15000；
- 吞吐率（MB/秒）:≥800Mbps；
- 每秒认证数（TPS）:≥15000。

**7. 移动签名服务**

支持移动安装包的签名与验证。

支持 RSA 和 SM2 双算法。

支持对数据、文件制作数字签名，签名结构符合 PKCS#7 标准；支持验证符合 PKCS#7 标准的签名结果。

支持对数据制作数字签名，签名结构符合 PKCS#1 标准；支持通过证书导入、证书配置方式验证符合 PKCS#1 标准的签名结果。

使用证书进行数字签名，接收者可验证签名，而其他任何人都不能伪造签名。

使用证书进行完整数字签名，签名结果中包含签名时的全部证书状态信息，接收者可在生成后的任意时间验证，而其他任何人都不能伪造。

支持居民身份证网上副本鉴真应用。

对重要数据、文件制作数字签名，如果验证签名失败，说明数据的完整性遭到破坏。

对操作行为（数据形式）制作数字签名，签名者事后不能否认自己的签名。

支持对数据、文件制作数字信封，信封结构符合 PKCS#7 标准；支持解密符合 PKCS#7 标准的信封结果。

对重要数据、文件制作数字信封，通过双层加密技术保障数据的私密性。

支持对签名、加密证书进行全面验证。

内置双机热备系统，采用主备机模式。

支持对硬件资源和业务能力进行实时监控，并且可以按年、月、日查看监控历史，同时可以根据年、月、日统计历史业务量。

支持对硬件资源和业务能力进行预警，产品支持自定义预警阀值，超过预警阀值时，系统会通过邮件或 SYSLOG 协议发送预警信息。

兼容性要求：支持完全兼容现有应用改造模式，要求现有已完成对接的应用系统，

在 APP 以及应用服务端不做任何调整的前提下，完成对接工作。

性能要求：

- 算法：SM2 密钥长度：256 bits；
- 数字签名：≥6200 次/秒；
- 签名验证：≥6000 次/秒；
- 制作信封：≥3300 次/秒；
- 解密信封：≥3500 次/秒。

**8. 空中发证服务**

提供空中发证服务，对接证书安全存储服务，实现证书的远程申请、自动下载、更新等操作。

支持不同厂商硬件 KEY 的驱动库，提供硬件适配能力。

服务内容包括证书安全存储管理服务：

- 要求证书存放于终端安全加密区域，满足公安部下发的《全国移动警务 PKI 空中发证技术方案》相关要求；
- 支持基于设备信息的密码模块注册授权；
- 具备密码模块授权动态控制功能；
- 支持密码模块的在线管理、统计和历史记录查询功能；
- 支持基于终端信息的终端认证功能；
- 与 PKI 服务、VPN 服务对接，实现证书的获取和写入、更新、删除服务；
- 提供终端密码模块、身份信息、认证信息等的综合管理和审计；
- 要求最大并发连接数：≥450；密码模块授权速率：≤100ms；身份证校验速率：≤500ms；设备认证速率：≤100ms。

### 2.3.8.2 集中管控服务需求

需提供移动警务统一运营服务，提供服务注册、服务发现、资源管理、能力编排、监控预警、数据配置、页面配置、服务运维、智能调度的能力，服务具备：

- 遵循公安部移动警务集中管控建设规范；
- 制定并提供管控接口接入能力,主要包括所有具有控制能力的防火墙、IPS 设备、边界设备、VPN 设备、MDM、资源管理服务、MAM、PKI 等开放的管控能力。提供自动化的管控指令下达和人工干预的指令下达能力，管控指令需根据具体的预警信息可自由组合。提供单个指令和指令集的下发和执行状态采集能力。人

工干预的指令下达经过可自定义的流程审批后，才可以进行实施；

- 需要完成对于 SIM 卡、云服务、网络带宽、发布服务、总线管理、公共基础服务、边、端资产、边缘计算、跨网云桌面、开发管理服务、数据资源的统一集中管控，可以实现资源接入、资源上架、资源申请、资源审批、资源回收、资源下架的全过程管理；
- 对于采集的数据按照规则进行分级、分类存储，实现高效的数据查询访问，支持自定义存储的需求、频度、位置等。完成性能指标类、复杂对象数据、资源关系类、关系型数据统一管理能力；
- 提供针对用户、业务应用系统、设备等的安全审计功能，以及对异常事件的追踪。主要包括：用户行为审计，即用户信息、访问的资源、访问的时间等；业务应用系统审计，即应用系统信息，数据传输流量、传输时间、传输单位等；设备运行审计；异常行为审计等；按时间段、应用系统、用户单位分析统计用户行为、业务应用系统数据传输、异常行为。通过数据可视化的呈现方式，以图表等形式直观展示安全数据，帮助安全管理员快速了解安全事件；
- 支持针对于关键字而对日志进行监控告警，多维度多指标，精确监控重要日志，实时产生关键字类型告警，分成三个级别按最高级进行告警，支持设置当系统所监控的日志文件中存在指定的关键字（支持正则表达式）时，系统能够产生告警，并且能够设置告警抑制的条件，配置项可进行高级配置使其更加精确的对于重要日志进行监控告警；
- 提供系统安全审计功能，安全审计的内容应记录系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用等。

#### 2.3.8.3 统一安全运维服务需求

提供一站式的日志数据管理工具，集日志收集、数据分析以及数据视图化功能，帮助用户提升运维、运营效率，快速查找和定位问题，辅助在线业务状态实时监控、业务异常原因定位、业务日志数据统计分析等场景。能够对各类应用系统的重要日志进行统一收集和管理，并能够根据特定的日志内容产生告警消息，为后期的运维工作提供有力的分析工具，协助运维人员分析系统故障，快速、准确地进行故障定位，提高运维效率。

需要完成所有管控资源的实时数据监控，并将数据存入态势感知中心下的数据采集器，提供态势感知的原始计算数据。

提供对现有的网络设备、主机/虚拟机、数据库、中间件、存储、业务应用等各类

云资源的监控管理，提供面向业务应用用户体验监测能力，并提供故障告警、性能数据、监控展示的集中化管理。

提供网络监控管理工具，面向网络运维人员，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。

需具备应用情况的实时监测，从而调整负载能力，可自动向活跃用户倾斜，在资源动态调整的情况下提高用户响应速度。

提供各运维工具和被管设备资源之间联络通讯的统一通道，并通过模块和插件的技术让各运维工具自由扩展采控能力，而不用关注底层的通讯和调度技术，只需要按照采控模块约定的规范编写采控脚本，并组织成策略下发给相应代理，对结果数据进行处理，即可完成机器数据采集、配置变更发布和资源操作控制。

系统提供全局网络拓扑与分层网络拓扑，全局拓扑显示所有的网络设备及关系。分层网络拓扑支持通过拓扑逐层建立组合的方式，支持构建骨干网拓扑展示，也可以根据业务管理场景进行拓扑构建。

提供可以用户自主配置的数据监控规则的能力基于用户自主配置的监控规则，提供用户自主配置监控页面的能力。

提供实时监控接入终端的安全状况、网络连接情况、系统和业务应用的运行情况；实时监控接入平台的运行状况，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，监控接入平台当前运行总体情况；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。

#### 2.3.8.4　全业务态势感知服务需求

安全风险和管控能力覆盖各个网络内的应用、终端、用户行为、服务、证书等，通过多形式的数据接入能力，通过大数据挖掘对风险进行实时预警，同时提供对应的自动化和手动的管控能力，及时控制预警信息对应的管控对象。

提供从网络系统、主机服务器、数据库、应用、安全等几方面的运行状况的集中展示管理平台，平台需提供当前运行一览视图、业务一览视图、业务监测视图、网络监测视图、机房展现视图等多种监测视图来查看当前系统的整体运行情况。

对告警事件进行统一的处理和分析，将移动警务环境中产生的异构、复杂且关联的事件信息通过集中的处理平台进行格式化、过滤、归并和关联分析，并将处理结果发送

给管理人员，帮助管理人员对各种事件进行有效的分析和后续处理。

对接感知数据智能采集器，获取态势感知存入的实时结果。

需要针对所有感知结果，进行实时计算，并可进行资源扩容、服务重启、访问限流、带宽调整、服务下线的能力。

需具备应用组合的能力，可进行 API 编排，提供多个注册服务的编排应用，完成业务需求的快速响应。

系统支持针对周期性的日常运维工作针对巡检、日清、合规、跑批和特定时间上线扩容等周期性或一次性执行的作业，可根据要求灵活设置定时执行策略。

支持通过应用建模，将各资源与应用建立关系。获取资源后，从用户体验、告警情况、性能负载 3 个维度进行健康度计算，同时结合对资源状态等维度的监控，从而对应用的健康状况进行有效的评估。系统能够根据故障源、故障源和配置项的关系以及当前配置项状态等因素，展现发生故障的配置项的健康状态；支持通过颜色变化、箭头来表示受影响的资源以及影响关系。

对接数据采集器，获取集中管控服务的原始数据。

所有感知计算结果的数据，需要实时存入统一运维下的数据采集器，提供统一运维模块的前置结果。

具有灵活展现和方便查找的告警分析功能，在告警功能中，可以详细显示和还原用户，应用的请求，并且可以设定策略。在违反某种策略的情况下，立即启动相应事件响应机制，支持通过联动安全设备、应用软件的管控能力来进行异常控制指令的自动下发，确保异常行为发生的时候，能在报警的同时，系统做出相应的反应来进行控制。

支持机器学习、深度学习等技术，提高自动化分析的准确性，能够更快速地发现和识别各种安全威胁和漏洞。

能够实现秒级响应，以满足紧急事件的及时处理需求，具有很高的响应性能和可靠性。

#### 2.3.8.5　移动警务终端安全管理服务需求

终端安全管理服务移动警务终端安全管控的组件，在新任务书和技术规范的要求上，其作为边、端安全接入和管理的重要组成部分，需在原有针对移动警务智能终端的管控基础上进一步延伸到多终端和多系统的管控。

按照边、端技术规范，面向边、端资产接入和管理服务提供多终端类型不同场景下的管控服务能力。

- 提供支持主动协议对接和协议文件自适应等模式下的管控对接技术手段来实现不同类型的终端和系统的快速管控接入，同时支持自定义管控项。
- 支持云端部署和边缘网关部署的形式，通过云、边联动实现对边缘网关和扩展类终端的管控。
- 根据边、端安全管控的技术标准，针对不同类型的终端设备的管控要求，与边、端资产接入和管理服务整合，实现对安全接入网关、直连终端、扩展终端的分级管控。
- 支持提供配置，实现管控策略在云端、网关端的二级缓存和修改，实现云-端、云-边-端的分发管理，同时支持根据配置实现边、端管控信息的层级上报和直连上报模式。

服务期内提供适配终端服务，终端类型包括且不仅限于安卓智能终端、鸿蒙系统、嵌入式系统终端、Linux 智能终端等。

其他终端的管控要求根据不同的网关类型和终端类型不同的对接方案和预置方案，作为预置到智能终端的管控能力的需求，具体要求如下：

- 提供移动终端注册时警员的身份信息与移动终端、数字证书、SIM 卡统一绑定，可通过自动读取证书信息等手段完成快速注册激活；
- 提供终端、SIM 卡分离自动锁定终端服务；
- 提供移动终端安全监控组件应以安全方式获取管控策略；
- 提供移动终端截屏功能、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。可根据策略内容，内部存储的数据进行擦除；
- 提供移动终端能够识别用户区域，并根据区域对终端 APN 参数、无线 VPN 客户端参数进行自动配置；

- 提供移动终端定期检测终端的操作系统版本、SIM/USIM 卡、终端密码模块、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；
- 提供移动终端未经许可更换 SIM 卡后，可自动上传终端的相关位置信息等；
- 提供移动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、无线网卡芯片型号、蓝牙芯片型号、NFC 芯片型号、定位芯片型号等；
- 提供移动终端支持终端 ROOT 监测功能，终端被 ROOT 后上报后台；
- 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、无线网络使用率、移动数据网络使用率等；
- 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、WLAN 配置推送、VPN 配置推送、APN 配置推送、SSO 配置推送与验证证书推送能力，实现对终端的远程控制和参数配置，终端执行管控策略后上报执行结果的目标；
- 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；
- 提供植入操作系统 ROM 服务；
- 与移动服务总线系统对接，开放所有终端开发能力。

#### 2.3.8.6 移动警务应用监管服务需求

移动警务应用监管服务是移动警务终端业务应用安全监测的组件，在新任务书和技术规范的要求上，需新增算力资源管理对边缘和扩展类终端上所运行的应用的监测能力，作为统一的应用监测服务，需同时满足对移动警务智能终端的上业务应用的监测、边缘网关、扩展类终端上业务应用和算力资源的运行监管的能力。同时作为算力资源管理的核心基础，算力资源管理在此基础上结合业务需求，对算力进行实时的调度和管理，在原有移动警务终端业务监管的基础上进一步延伸到多终端和多系统联动，且服务模式由原来的监测监管，进一步向业务服务基础延伸。

按照边、端技术规范，面向边缘算力服务的算力调度提供网关、扩展类终端上业务运行的状态、资源损耗、预计业务运行的周期等基础数据，以辅助算力调度中心对算力能力实时的调配。

提供支持不同类型的终端、不同类型的操作系统上的应用的运行行为的数据监测能力，并根据集中管控的技术标准实时上报业务运行状态。

提供多形态技术对接手段，以满足不同的业务接入形态，包括且不仅限于开放统一的数据接入服务能力、统一的采集中间件等，能够满足接入平台的终端类型和业务类型的监测需求。

统一采集中间件能够采集的数据，需要满足集中管控对行为数据的日志规范要求。

支持云端部署和边缘网关部署的形式，通过云、边联动实现对边缘网关、扩展类终端上的业务运行状态的采集上报。

根据边、端安全管控的技术标准，针对不同类型的数据监测要求，与算力管理服务能力整合，实现对网关、直连终端、扩展终端上的业务服务运行的的分级监测与上报。

支持提供配置，实现监测数据在云端、网关端的二级缓存和上报，支持根据配置实现边、端管控信息的层级上报和直连上报模式。

服务期内提供适配终端应用服务，终端类型包括且不仅限于安卓智能终端、嵌入式系统终端、Linux 智能终端等。

其他终端得监测根据不同的网关类型和终端类型、业务形态制定不同的监测方法，作为预置到智能终端的业务监测的需求，具体如下：

- 提供移动终端应用红/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；
- 提供移动终端对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；
- 提供所有移动终端安全运行环境，对移动警务应用提供隔离、网络切换、运行保护、数据防泄漏等必要保护措施；
- 提供移动终端不允许禁止卸载列表中的应用被卸载；
- 提供应用加固功能：给应用提供签名校验等保护；
- 提供应用运行信息上报服务，包括但不仅限于登录失败监测、互联网联通监测、应用的使用情况，包括时长、流量、异常信息等。

#### 2.3.8.7 多因子认证服务需求

与统一门户对接，实现多因子认证服务，提供证书的验证、PIN 码登陆、人脸识别登陆、指纹登陆、账号密码登录等能力，支持可配置一种认证方式或者多种认证方式的集合。

提供基于人脸识别、指纹识别、数字证书验证几种登陆验证方式。

提供集中指纹识别服务，用户注册时采集个人指纹信息，服务端存储指纹，并对外提供指纹验证的服务。

提供人脸识别登录服务，提供人脸采集和人脸验证服务。

与统一用户服务对接，获取用户名密码验证形式，账号密码支持自定义形式，并对外提供账号密码登录的服务。

支持跨终端跨系统的多因子认证服务。

### 2.3.9 移动警务基础安全设施服务需求

为保证市局的 APN/VPDN 接入的安全性以及各类接入区域的安全性，同时满足移动警务统一运营的目的，要求基础设施安全服务包含的所有软硬件设施需按照统一运营服务要求提供数据接口，达到集中管控、统一运维、态势感知等系统方面能力，**基础设施安全服务所涉及的设备应具有原厂授权及原厂售后服务。**

#### 2.3.9.1 移动互联网安全防护服务需求

移动互联网安全防护服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

提供边界网络防护服务：网络层吞吐量不低于 10Gbps，应用层吞吐量数据的安全防护能力不低于 3Gbps，并发连接数不低于 220 万个，新建连接数不低于 15 万次/秒，不少于 10 个千兆电口，不少于 4 个千兆光口，要求满配光模块，要求在三年内持续更新对最新威胁的防护能力，需提供可基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组等方式的访问控制能力，具备长连接功能并可以配置连接时长；需提供支持模拟策略匹配的访问控制规则，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，以具备快速排查故障的能力；支持自动生成综合安全风险报表；支持与网络审计服务实现认证联动的能力；支持与终端检测响应服务实现联动；要求设备冗余，支持开放网络数据和防护接口服务，支持第三方调用。

提供入侵防御服务：网络层吞吐量不低于 10Gbps，吞吐数据的入侵防御能力不低于 4Gbps，并发连接数不低于 220 万个，入侵防御服务新建连接数不低于 12 万次/秒；不

少于 10 个千兆电口，不少于 4 个千兆光口，要求满配光模块，具备对服务器和客户端的漏洞攻击防护，支持 XSS 攻击、SQL 注入等 Web 攻击行为的有效防护能力，支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，且支持自定义封锁时间，支持提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，支持根据国家/地区来进行地域访问控制以保障业务访问安全性。具备与同安全态势感知服务联动能力，产品支持以标准 SYSLOG 形式上传到态势感知平台，供态势感知系统进行深度关联分析并对恶意威胁实现联动封锁；要求设备冗余，支持开放数据和防御服务接口，支持第三方调用。

提供网络审计服务，网络审计能力不低于 2.5Gbps，并发连接数不低于 70 万个，网络审计服务的新建连接数不低于 1.5 万次/秒；提供网络实时监控服务，提供应用管理服务，提供 URL 管理服务，提供邮件管理服务，提供网页审计服务，支持记录全部或者指定类别 URL、网页标题等信息，能审计记录网页正文内容，支持关键字订阅服务，支持自定义报表服务，要求满足设备冗余，支持面向第三方系统提供数据同步服务。

提供抗 DDOS 服务，网络吞吐服务能力不低于 10Gbps，要求满足设备冗余，提供异常流量检测服务，网络层 Flood 检测、应用层 Flood 检测、畸形包 DDoS 检测，提供异常流量清洗服务，支持黑白名单防护功能，提供用户管理服务，支持配置管理、审计管理和账号管理权限设定，支持口令复杂度设定，支持可信管理主机设定，不少于 2 套。

提供 APT 防御服务，防御服务能力不低于 1Gbps，具备静态扫描和动态检测能力，具备多格式分析能力，对远程代码执行、异常 http 下载、C&C 定时任务、DGA、DNS 隐秘隧道、文件威胁等进行有效检测。能够和安全态势感知服务结合形成关联分析报告，提供针对攻击事件的攻击链分析、入口溯源服务，能够不限次进行响应，并提供分析结果，能够对指定的 URL/域名/IP/MD5/文件进行分析，支持面向第三方开放预警信息服务。

提供脆弱性扫描服务，主机漏扫最大并发 IP 数不低于 300，Web 漏扫最大并发 URL 数不低于 10，实现根据扫描结果提供专业、有效的安全分析和修补建议。

提供 WAF 防护服务，网络层吞吐量不低于 20Gbps，HTTP 应用层吞吐量不低于 1Gbps，HTTP 新建连接数不低于 150000，HTTP 并发连接数不低于 220 万，内存大小不低于 8G，硬盘容量不低于 128GB 接口不少于 6 千兆电口+2 万兆光口 SFP+，满配光模块。

提供应用负载均衡服务，不少于 6 个千兆电口，不少于 4 个千兆光口，吞吐量不低于 6Gbps，并发连接数不低于 500 万条，每秒新建连接数不低于 18 万。要求含服务器负载均衡，多链路负载均衡，全局负载均衡，智能 DNS，DNS 代理，TCP 单边加速，应用系

统加速（Cache，SSL 协议卸载，TCP 链接复用等）。所有功能及用户数没有许可限制。

提供基于安全基座的 VPN 服务，支持并发用户数不少于 1 万终端；需采用标准 SSL、TLS 协议提供虚拟隧道网络服务，提供基于 TCP、UDP、ICMP 等 IP 层以上的协议的应用服务；提供的 VPN 服务需要支持现有移动警务认证方式，包括但不限于 INSE 模式下国密 SM2 证书结合认证、SIM 卡贴膜卡国密 SM2 证书结合认证、SIM 卡贴膜卡商密 RSA 证书结合认证，支持伪装服务器地址功能，VPN 服务可以将真实的服务器地址伪装成域名形式。

#### 2.3.9.2 移动互联网管控服务需求

移动互联网管控服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

提供安全感知服务，防御服务能力不低于 5Gbps，要求具有资产发现与风险管控服务，通过自动或人工的方式识别到资产的风险和脆弱性，可输出风险评估日报、周报、月报，威胁情报等服务，可提供最新威胁情报来源，同时对新出现的漏洞、病毒、攻击行为等在网络内进行自动检查，并以月为单位提供分析报告；威胁实时监测服务，具备机器学习和 UEBA 能力，对来自外部和内部的攻击行为、异常访问、横向扩散等行为有效识别，及时发现威胁，并能够通过自动化的流程触发安全防护服务或终端检测响应服务实现闭环处理；勒索病毒专项检查服务，通过非破坏的方式对网络内的勒索病毒防控能力进行评估，对各主流勒索病毒家族及变种进行检。对于识别到的风险能够通过自动化的流程触发终端检测响应服务进行整改；通报预警服务，针对识别到的风险和事件能够通过工单平台展示，并通过邮件、短信等方式推送到对应责任人；支持面向第三方开放数据同步服务和安全管控接口。

提供防病毒服务：计算机终端安全防护数量不低于 1000 个，具备全网终端安全可视，终端资产管理，统一策略下发，微隔离流量可控，终端间访问关系可视，全网终端威胁检测，终端漏洞补丁管理，勒索病毒防护服务，终端基线检测管理，多维度威胁检测服务，Windows/Linux 终端合规检查服务，全网威胁定位，提供 WebShell 事件处理服务，日志报表分析等，支持面向第三方提供病毒预警信息服务。

提供日志审计服务，提供至少 500 个主机审计能力，处理性能不低于 10000 条/秒；支持获取各种主流网络及数据库访问行为，支持 SYSLOG、WMI、SNMP trap、文本、JDBC/ODBC 和 LAS-1000 专用协议等协议事件日志，支持通过日志导入、SFTP、SMB 等协议获取各类文件型日志，支持会话数据解码和分析，支持普通以太头解析、支持 PPPoE、

VLAN、VLAN QinQ、支持 TCP、UDP、ICMP、ICMPv6、SCTP、IGMP 等，支持 HTTP、DNS、邮件等，支持面向第三方提供日志数据和审计结果数据的同步服务。

提供堡垒机服务，需提供不少于 50 个支撑资源授权服务，需提供通过多种协议的服务，如字符协议 SSHv1、SSHv2、Telnet，图形协议：RDP、VNC，文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板等；支持图形协议并发支撑数不少于 300 个，支持字符协议并发支撑数 1500 个。可提供支撑人员单点登录、用户权限细粒度授权及访问控制、支撑过程审计等功能，提供从 Web 页面设置多端口绑定服务。

提供身份认证服务，实现登录人员的实名认证。

集中管控系统提供数据采集的标准和相关的技术能力，面向平台上所有的应用和平台系统提供数据接入服务和管控接口接入能力。

提供日志审计和服务能力，并面向公安部上报相关数据。

提供自动化的管控指令下达和人工干预的指令下达能力。

提供单个指令和指令集的下发和状态采集能力。

提供短信网关服务，配合身份认证系统发送随机认证密码短信，短信数量每月不低于 100 万条，要求满足设备冗余。

提供网络探针服务，用于平台内部设备状态获取以及设备管理，采集所在区域所有设备的运行状态，包括 CPU、内存、网络等使用情况以及由操作系统产生的各类异常告警信息等:将通 SYSLOG、SNMP、Telnet、ICMP 等方式获取到的信息传输给集中管控系统:性能要求:千兆电口不低于 6 个，USB 接口不低于 2 个,COM 接口不低于 1 个；稳定性运行时间(MTBF):>50000 小时；网络吞吐量不低于 800Mbps；支持不低于 200 个采集单元。

提供数据探针服务，用于平台内部设备登录记录、认证记录、社会账号、ICMP 协议、TCP 会话、UDP 会话等原数据提取:支持与集中管控系统对接，能够向平台端上报所有日志信息，能够接收平台端下发的控制策略；性能要求:千兆电口不低于 6 个，千兆光口不低于 2 个,USB 不低于 2 个，COM 接口不低于 1 个；稳定性运行时间(MTBF):>50000 小时;数据包实时采集和分析不低于 2Gbps 处理能力，TCP/UDP 会话处理能力不低于每秒 3000;支持探针设备横向扩展:

提供多种终端认证机制，支持密钥认证、证书认证、Token 认证等主流认证方式，满足不同安全等级设备的认证接入需求。

提供动态密钥管理服务，支持第三方系统通过标准接口为设备生成临时访问凭证，实现安全可控的短期接入授权。

提供终端嵌入式认证服务组件，支持多类型终端的快速接入认证。

提供自定义认证插件管理能力，支持第三方认证逻辑以插件形式接入平台。

提供认证凭证的生命周期管理，支持对设备证书、密钥等凭证进行全流程管理，包括且不仅限于颁发、吊销、更新、校验等操作。

提供设备认证状态的可视化监控与管理，支持实时查看设备认证成功/失败状态，并可将认证结果同步至第三方业务系统。

#### 2.3.9.3 移动互联网可信服务需求

提供统一安全基座接入服务。安全基座负责对其承载的原生应用和轻应用提供安全防护。同时提供身份认证、应用运行、权限控制、数据安全、终端监测和加密传输等。支持原生应用和轻应用的接入和运行。

提供统一的安全链路接入服务，提供基于国密算法创建的加密传输通道，用于业务数据的安全传输。

提供国产密码基础设施服务，包括云密码机服务为应用提供相应的密码服务，密码设施具备国家密码管理局商用密码检测认证中心颁发的商用密码产品认证证书。

提供基于国密基础的设备证书的认证服务能力，并与安全基座联动，提供设备入网的管控。

#### 2.3.9.4 联网服务区物联网接入控制服务需求

联网服务区物联网接入控制服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

提供边界网络防护服务：网络层吞吐量不低于 65Gbps，应用层吞吐量数据的安全防护能力不低于 40Gbps，并发连接数不低于 1600 万个，新建连接数不低于 55 万次/秒，不少于 4 个 40G 光口，4 个千兆电口，8 个万兆光口，并要求满配光模块；要求在三年内持续更新对最新威胁的防护能力，需提供可基于源/目的 IP，源端口，源/目的区域，用户（组），应用/服务类型，时间组等方式的访问控制能力，具备长连接功能并可以配置连接时长；需提供支持模拟策略匹配的访问控制规则，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，以具备快速排查故障的能力；支持自动生成综合安全风险报表；支持与网络审计服务实现认证联动的能力；支持与终端检测响应服务实现联动；要求设备冗余，支持开放网络数据和防护接口服务，支持第三方调用。

提供入侵防御防护服务：网络层吞吐量不低于 65Gbps，数据的入侵防御能力不低于

10Gbps，并发连接数不低于 1600 万个，入侵防御服务新建连接数不低于 55 万次/秒；不少于 4 个 40G 光口，4 个千兆电口，8 个万兆光口，要求满配光模块，具备对服务器和客户端的漏洞攻击防护，支持 XSS 攻击、SQL 注入等 Web 攻击行为的有效防护能力，支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，且支持自定义封锁时间，支持提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，支持根据国家/地区来进行地域访问控制以保障业务访问安全性。具备与同安全态势感知服务联动能力，产品支持以标准 SYSLOG 形式上传到态势感知平台，供态势感知系统进行深度关联分析并对恶意威胁实现联动封锁；要求设备冗余，支持开放数据和防御服务接口，支持第三方调用。

提供 LNS 路由器服务，单台支持 L2TP 隧道数不低于 5 万，双主控，双交换网板，不低于三个电源模块，交换容量不低于 195.24Tbps，包转发率不低于 172800Mpps，不低于 6 个 40G 光口，10 个万兆光口，要求满配光模块，要求满足设备冗余。

提供 AAA 服务，提供不低于 5 万用户认证，提供第三方接口，包含且不仅限于用户信息的查询、写入、更新删除等接口服务，同时要满足对接运营商物联网平台，实现机卡绑定，满足冗余。

提供分局及交管总队物联网防火墙服务，要求网络层吞吐量不低于 20Gbps，应用层吞吐量不低于 9Gbps，并发连接数不低于 200 万，HTTP 新建连接数不低于 9 万，数量不少于 17 台，单台配置万兆光口不少于 2 个，千兆光口不少于 8 个。

#### 2.3.9.5 联网服务区接入控制服务需求

根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

提供 AAA 服务，提供不低于 6 万用户认证，提供第三方接口，包含且不仅限于用户信息的查询、写入、更新、删除等接口服务，要求满足冗余。

提供边界网络防护服务：网络层吞吐量不低于 40Gbps，应用层吞吐量数据的安全防护能力不低于 25Gbps，并发连接数不低于 420 万个，新建连接数不低于 30 万次/秒，不少于 16 千兆电口，少于 6 个万兆光口，并要求满配光模块；要求在三年内持续更新对最新威胁的防护能力，需提供可基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组等方式的访问控制能力，具备长连接功能并可以配置连接时长；需提供支持模拟策略匹配的访问控制规则，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，以具备快速排查故障的能力；支持自动生成

综合安全风险报表；支持与网络审计服务实现认证联动的能力；支持与终端检测响应服务实现联动；要求设备冗余，支持开放网络数据和防护接口服务，支持第三方调用。

提供入侵防御防护服务：网络层吞吐量不低于 18Gbps，数据的入侵防御能力不低于 7Gbps，并发连接数不低于 400 万个，入侵防御服务新建连接数不低于 30 万次/秒；不少于 4 个千兆电口，不少于 4 个千兆光口，不少于 4 个万兆光口，并要求满配光模块，具备对服务器和客户端的漏洞攻击防护，支持 XSS 攻击、SQL 注入等 Web 攻击行为的有效防护能力，支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，且支持自定义封锁时间，支持提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，支持根据国家/地区来进行地域访问控制以保障业务访问安全性。具备与同安全态势感知服务联动能力，产品支持以标准 SYSLOG 形式上传到态势感知平台，供态势感知系统进行深度关联分析并对恶意威胁实现联动封锁；要求设备冗余，支持开放数据和防御服务接口，支持第三方调用。

提供 APT 防御服务，防御服务能力不低于 3Gbps，具备静态扫描和动态检测能力，具备多格式分析能力，对远程代码执行、异常 http 下载、C&C 定时任务、DGA、DNS 隐秘隧道、文件威胁等进行有效检测。能够和安全态势感知服务结合形成关联分析报告，提供针对攻击事件的攻击链分析、入口溯源服务，能够不限次进行响应，并提供分析结果，能够对指定的 URL/域名/IP/MD5/文件进行分析，支持面向第三方开放预警信息服务。

提供网络审计服务，网络审计能力不低于 5.5Gbps，并发连接数不低于 200 万个，网络审计服务的新建连接数不低于 4 万次/秒；提供网络实时监控服务，提供应用管理服务，提供 URL 管理服务，提供邮件管理服务，提供网页审计服务，支持记录全部或者指定类别 URL、网页标题等信息，能审计记录网页正文内容，支持关键字订阅服务，支持自定义报表服务，要求满足设备冗余，支持面向第三方系统提供数据同步服务。

提供安全准入服务，要求网络层吞吐量不低于 1.5Gbps，提供不低于 600 用户的安全准入服务，要求满足设备冗余，提供接入认证服务，服务类型包括但不限于 802.1x 认证、MAB 认证、单点登录认证等，提供实时监控服务，提供终端非法外联安全管控服务，提供资产管理服务，提供终端管理服务，支持识别终端操作系统版本、系统补丁安装情况，提供准入联动服务，能够和分局/交管总队层面安全准入服务进行联动，从而形成全局精细化终端安全管理和联动处置，支持面向第三方提供安全准入验证数据同步。

提供 LNS 路由器服务，支持 L2TP 隧道数不低于 6 万，设备接口不低于 8 个万兆光口，20 个千兆光口，要求满配单模光模块，要求满足冗余。

提供区分局及交管总队安全准入服务，要求网络层吞吐量不低于500Mbps，提供不低于5220用户的安全准入服务，要求满足设备冗余，提供接入认证服务，服务类型包括但不限于802.1x认证、MAB认证、单点登录认证等，提供实时监控服务，提供终端非法外联安全管控服务，提供资产管理服务，提供终端管理服务，支持识别终端操作系统版本、系统补丁安装情况，提供准入联动服务，能够和分局/交管总队层面安全准入服务进行联动，从而形成全局精细化终端安全管理和联动处置，支持面向第三方提供安全准入验证数据同步，数量不少于17套。

提供区分局及交管总队APT检测服务，防御服务能力不低于1Gbps，具备静态扫描和动态检测能力，具备多格式分析能力，对远程代码执行、异常http下载、C&C定时任务、DGA、DNS隐秘隧道、文件威胁等进行有效检测。能够和安全态势感知服务结合形成关联分析报告，提供针对攻击事件的攻击链分析、入口溯源服务，能够不限次进行响应，并提供分析结果，能够对指定的URL/域名/IP/MD5/文件进行分析，支持面向第三方开放预警信息服务，数量不少于17套。

#### 2.3.9.6 联网服务区管控服务需求

联网服务区管控服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

##### 2.3.9.6.1 提供防病毒服务

计算机终端安全防护数量不低于1000个，具备全网终端安全可视，终端资产管理，统一策略下发，微隔离流量可控，终端间访问关系可视，全网终端威胁检测，终端漏洞补丁管理，勒索病毒防护服务，终端基线检测管理，多维度威胁检测服务，Windows/Linux终端合规检查服务，全网威胁定位，提供WebShell事件处理服务，日志报表分析等，支持面向第三方提供病毒预警信息服务。

##### 2.3.9.6.2 提供安全感知服务

提供安全感知服务，防御服务能力不低于36Gbps，要求具有资产发现与风险管控服务，通过自动或人工的方式识别到资产的风险和脆弱性，可输出风险评估日报、周报、月报，威胁情报等服务，可提供最新威胁情报来源，同时对新出现的漏洞、病毒、攻击行为等在网络内进行自动检查，并以月为单位提供分析报告；威胁实时监测服务，具备机器学习和UEBA能力，对来自外部和内部的攻击行为、异常访问、横向扩散等行为有效识别，及时发现威胁，并能够通过自动化的流程触发安全防护服务或终端检测响应服务实现闭环处理；勒索病毒专项检查服务，通过非破坏的方式对网络内的勒索病毒防控

能力进行评估，对各主流勒索病毒家族及变种进行检。对于识别到的风险能够通过自动化的流程触发终端检测响应服务进行整改；通报预警服务，针对识别到的风险和事件能够通过工单平台展示，并通过邮件、短信等方式推送到对应责任人；支持面向第三方开放数据同步服务和安全管控接口。

#### 2.3.9.6.3 提供流量监测服务

提供满足公安无线链路管控要求的链路资源监管服务，实现公众移动通信网专用传输链路链路资源的统一监管，包括但不限于链路流量采集分析、链路监测、路由管控、用户管理、信息汇总和级联上报等。支持采集 LNS 路由器的接口流量，满足对源目的地址、端口等报文元数据进行分析的服务要求。支持与 LNS 路由器联动，满足获取 IP 地址池及下发路由控制策略的服务要求。支持与 AAA 服务器联动，满足查询用户身份标识、终端身份标识、IP 地址等用户管理信息的服务要求。支持对 5G 物网专线链路的链路监管，提供链路基本信息、链路切片信息、终端信息等信息查询服务。支持按照标准的信息汇总和级联上报接口，实现向无线管控中心的级联上报。

#### 2.3.9.6.4 提供数据探针服务

提供数据探针服务，用于平台内部设备登录记录、认证记录、社会账号、ICMP 协议、TCP 会话、UDP 会话等原数据提取:支持与集中管控系统对接，能够向平台端上报所有日志信息，能够接收平台端下发的控制策略；性能要求:千兆电口不低于 6 个，千兆光口不低于 2 个,USB 接口不低于 2 个，COM 接口不低于 1 个；稳定性运行时间(MTBF):>50000 小时;数据包实时采集和分析不低于 2Gbps 处理能力，TCP/UDP 会话处理能力不低于每秒 3000;支持探针设备横向扩展:

提供网络探针服务，用于平台内部设备状态获取以及设备管理，采集所在区域所有设备的运行状态，包括 CPU、内存、网络等使用情况以及由操作系统产生的各类异常告警信息等:将通 SYSLOG、SNMP、 Telnet、ICMP 等方式获取到的信息传输给集中管控系统:性能要求:千兆电口不低于 6 个，USB 接口不低于 2 个,COM 接口不低于 1 个;稳定性运行时间(MTBF):>50000 小时;网络吞吐量不低于 800Mbps;支持不低于 200 个采集单元。

提供潜伏威胁探针服务，用于平台对各种攻击行为以及网络威胁进行高精度的检测，在内网中对潜伏威胁流量的异常情况提供准确和有效的发现能力。性能参数：网络层吞吐量不低于 20Gbps，应用层吞吐量不低于 12Gbps，千兆电口不低于 4 个，万兆光口不低于 8 个。

#### 2.3.9.6.5 提供日志审计服务

1.提供日志审计服务，提供至少 500 个主机审计能力，处理性能不低于 10000 条/秒；提供不低于 8TB 数据硬盘；提供不少于 4 个千兆电口，4 个万兆光口；支持获取各种主流网络及数据库访问行为，支持 SYSLOG、WMI、SNMP trap、文本、JDBC/ODBC 和 LAS-1000 专用协议等协议事件日志，支持通过日志导入、SFTP、SMB 等协议获取各类文件型日志，支持会话数据解码和分析，支持普通以太头解析、支持 PPPoE、VLAN、VLAN QinQ、支持 TCP、UDP、ICMP、ICMPv6、SCTP、IGMP 等，支持 HTTP、DNS、邮件等，支持面向第三方提供日志数据和审计结果数据的同步服务。

2.数据库审计服务，最大硬件吞吐量不低于 5Gbps，最大数据库纯 SQL 流量不低于 800Mb/s，数据库实例个数：无限制，SQL 处理性能不低于 50000 条 SQL/s，日志检索性能不低于 1200000 条/秒。内存不低于 16G，硬盘容量不低于 128GB SSD+4TB SATA，冗余电源，不低于 6 个千兆电口。

数据库安全审计系统基于深度数据库协议解析技术，采用自动学习和智能分析模式，实现对数据库访问行为的全程监控、高危操作的实时告警和安全事件的审计追溯。帮助提升数据库访问行为的透明度，降低人工审计成本，真正实现数据库全业务运行可视化、日常操作可监控、危险操作可控制、访问行为可审计、安全事件可追溯。

#### 2.3.9.6.6 提供漏洞扫描服务

提供脆弱性扫描服务，主机漏扫最大并发 IP 数不低于 300 个，Web 漏扫最大并发 URL 数不低于 10 个，实现根据扫描结果提供专业、有效的安全分析和修补建议。

#### 2.3.9.6.7 提供堡垒机服务

提供堡垒机服务，需提供不少于 800 个支撑资源授权服务，图形运维最大并发数不低于 200 个，需提供通过多种协议的服务，如字符协议 SSHv1、SSHv2、Telnet，图形协议：RDP、VNC，文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板等；持图形协议并发支撑数不少于 300 个，支持字符协议并发支撑数 1500 个。可提供支撑人员单点登录、用户权限细粒度授权及访问控制、支撑过程审计等功能，提供从 Web 页面设置多端口绑定服务。

#### 2.3.9.6.8 提供移动身份认证网关服务

支持移动警务 CA 颁发的数字证书。

支持 RSA 和 SM2 双算法。

支持主路和旁路两种工作模式。

结合警用移动终端数字证书管理系统，可通过扫描二维码方式实现用户身份信息的漫游功能。

支持警员证书等多种证书类型的身份认证，对于公安未来定义的证书类型保持扩展设计，以便在新证书类型出现时能够无缝结合。

支持证书信息传递功能，能够根据不同的公安行业证书结构进行解析，如警员、岗位、机构等证书格式，将基本信息和扩展域信息传递给后台应用。

支持入门级访问控制，能够根据不同的证书类型，对应用的入门级访问进行许可控制，防止岗位和机构等证书对应用的越权使用。

能够根据公安的数字证书格式标准，获取警员的个人、群体、自定义信息。

支持将警员认证信息、属性信息、获取信息发至第三方应用系统。

支持基于用户角色的访问控制。

支持向业务系统传递属性信息。

支持 B/S、C/S 应用系统接入。

支持以 SYSLOG 标准方式发送证书登录日志。

支持 TOP N 功能。

支持双机热备，防止单点故障。

能够对管理员进行限制。管理员通过证书验证后方可获得集中认证网关管理系统的权限。

能够支持系统备份、恢复。

系统支持通过 OCSP 协议方式对证书状态进行验证，更实时、更准确。

系统支持通过证书基本属性、证书扩展属性、用户属性、时间、终端地址、硬件设备特征以及信任域进行业务系统的授权和访问控制，通过不同条件的组合做到灵活授权。

系统支持对后端业务系统负载，在不使用第三方负载均衡设备的情况下实现对业务系统的负载效果。

兼容性要求：支持完全兼容现有应用改造模式，要求现有已完成对接的应用系统，在 APP 以及应用服务端不做任何调整的前提下，完成对接工作。

性能要求：

新建连接速度（次/秒）:≥3000；

最大并发连接数:≥15000；

吞吐率（MB/秒）:≥800Mbps；

每秒认证数（TPS）:≥15000。

#### 2.3.9.6.9 提供移动签名服务

支持移动安装包的签名与验证。

支持 RSA 和 SM2 双算法。

支持对数据、文件制作数字签名，签名结构符合 PKCS#7 标准；支持验证符合 PKCS#7 标准的签名结果。

支持对数据制作数字签名，签名结构符合 PKCS#1 标准；支持通过证书导入、证书配置方式验证符合 PKCS#1 标准的签名结果。

使用证书进行数字签名，接收者可验证签名，而其他任何人都不能伪造签名。

使用证书进行完整数字签名，签名结果中包含签名时的全部证书状态信息，接收者可在生成后的任意时间验证，而其他任何人都不能伪造。

支持居民身份证网上副本鉴真应用。

对重要数据、文件制作数字签名，如果验证签名失败，说明数据的完整性遭到破坏。

对操作行为（数据形式）制作数字签名，签名者事后不能否认自己的签名。

支持对数据、文件制作数字信封，信封结构符合 PKCS#7 标准；支持解密符合 PKCS#7 标准的信封结果。

对重要数据、文件制作数字信封，通过双层加密技术来保障数据的私密性。

支持对签名、加密证书进行全面验证。

内置双机热备系统，采用主备机模式。

支持对硬件资源和业务能力进行实时监控，并且可以按年、月、日查看监控历史，同时可以根据年、月、日统计历史业务量。

支持对硬件资源和业务能力进行预警，产品支持自定义预警阀值，超过预警阀值时，系统会通过邮件或 SYSLOG 协议发送预警信息。

兼容性要求：支持完全兼容现有应用改造模式，要求现有已完成对接的应用系统，在 APP 以及应用服务端不做任何调整的前提下，完成对接工作。

性能要求：

算法：SM2 密钥长度：256 bits；

数字签名：≥6200 次/秒；

签名验证：≥6000 次/秒；

制作信封：≥3300 次/秒；

解密信封：≥3500 次/秒。

#### 2.3.9.6.10 提供空中发证服务

提供空中发证服务，对接证书安全存储服务，实现证书的远程申请、自动下载、更新等操作。

支持不同厂商硬件 KEY 的驱动库，提供硬件适配能力。

服务内容包括证书安全存储管理服务。

要求证书存放于终端安全加密区域，满足公安部下发的《全国移动警务 PKI 空中发证技术方案》相关要求。

支持基于设备信息的密码模块注册授权。

具备密码模块授权动态控制功能。

支持密码模块的在线管理、统计和历史记录查询功能。

支持基于终端信息的终端认证功能。

与 PKI 服务、VPN 服务对接，实现证书的获取和写入、更新、删除服务。

提供终端密码模块、身份信息、认证信息等的综合管理和审计。

要求最大并发连接数：≥450；

密码模块授权速率：≤100ms；

身份证校验速率：≤500ms；

设备认证速率：≤100ms。

#### 2.3.9.6.11 提供 DNS 服务

提供 DNS 服务，满足 11 万终端用户的使用。

### 2.3.9.7 联网服务区互联网隔离服务需求

联网服务区互联网隔离服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

1、提供负载均衡服务，要求吞吐量不低于 5Gbps，并发连接数不低于 300 万次，满足设备冗余；支持轮询、加权轮询、按主机加权轮询、优先级等算法；具备支持源 IP 等多种会话保持机制，具备跨虚拟服务的会话保持机制、具备将服务器负载状态投屏展示的能力，千兆电口不低于 6 个、千兆光口不低于 2 个，要求光模块满配。提供 2 台。

2、提供双单向光闸系统：内/外端机的背板带宽不低于 6Gbps，不低于 6 个千兆以太网口,单向光纤传输的 UDP 实际传输速率不低于 900Mbps,数据库同步每秒不低于 2000 条，单线程 FTP 文件摆渡方式每秒不低于 80Mbps，数量不低于 4 套，支持面向第三方实

时提供服务日志，提供配置及策略下发端口。

提供双单向光闸系统：内/外端机的背板带宽不低于 8Gbps，不低于 6 个千兆以太网口，不低于 2 个万兆光口，单向光纤传输的 UDP 实际传输速率不低于 2Gbps，数据库同步每秒不低于 10000 条，单线程 FTP 文件摆渡方式每秒不低于 100Mbps，数量不低于 2 套，支持面向第三方实时提供服务日志，提供配置及策略下发端口。

3、提供前置服务：支持 UDP 方式传输数据；文件同步功能，支持文件的同步，多级目录结构同步，可进行文件过滤；FTP 同步方式，可支持 30GB 大文件传输；数据库同步，支持触发器、全表、删除原表数据、时序等同步方式；支持数据库错误恢复功能，可对传输中的丢失数据进行恢复，支持数据库结构自动匹配及主从自动排序功能，快速进行业务配置；支持将审计信息或报警信息发送到集中监控系统统一管理，背板带宽不低于 6Gbps，数量不低于 4 套

提供前置服务：支持 UDP 方式传输数据；文件同步功能，支持文件的同步，多级目录结构同步，可进行文件过滤；FTP 同步方式，可支持 30GB 大文件传输；数据库同步，支持触发器、全表、删除原表数据、时序等同步方式；支持数据库错误恢复功能，可对传输中的丢失数据进行恢复，支持数据库结构自动匹配及主从自动排序功能，快速进行业务配置；支持将审计信息或报警信息发送到集中监控系统统一管理，背板带宽不低于 8Gbps，数量不低于 2 套

4、提供后置服务，支持 UDP 方式传输数据；文件同步功能，支持文件的同步，多级目录结构同步，可进行文件过滤；FTP 同步方式，可支持 30GB 大文件传输；与导入前置机配合实现数据库同步，支持触发器、全表、删除原表数据、时序等同步方式；支持数据库结构自动匹配及主从自动排序功能，快速进行业务配置；支持将审计信息或报警信息发送到集中监控系统统一管理。采用基于 HTTPS 安全协议的管理方式;支持 SYSLOG、SNMPX 协议，背板带宽不低于 6Gbps，数量不低于 4 套。

提供后置服务，支持 UDP 方式传输数据；文件同步功能，支持文件的同步，多级目录结构同步，可进行文件过滤；FTP 同步方式，可支持 30GB 大文件传输；与导入前置机配合实现数据库同步，支持触发器、全表、删除原表数据、时序等同步方式；支持数据库结构自动匹配及主从自动排序功能，快速进行业务配置；支持将审计信息或报警信息发送到集中监控系统统一管理。采用基于 HTTPS 安全协议的管理方式；支持 SYSLOG、SNMPX 协议，背板带宽不低于 8Gbps，数量不低于 2 套。

#### 2.3.9.8 联网服务区视频隔离服务需求

联网服务区视频隔离服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

1、提供负载均衡服务，要求吞吐量不低于40Gbps，并发连接数不低于8000万次，满足设备冗余；支持轮询、加权轮询、按主机加权轮询、优先级等算法；具备支持源IP等多种会话保持机制，具备跨虚拟服务的会话保持机制、具备将服务器负载状态投屏展示能力，千兆电口不低于4个、千兆光口不低于4个、万兆光口不低于4个，要求光模块满配，至少提供4台。

2、提供数据交换服务，应用吞吐量不低于750Mbps，图像传输性能线性不低于700Mbps,支持不少于350路D1传输能力，单路图像码率不低于20Mbps，万兆光口数不低于2个，要求满配光模块，支持标准SIP信令控制协议，支持GB/T 28181标准；数量不低于1套2台，支持面向第三方实时提供服务日志，提供配置及策略下发端口，提供配置及策略下发端口。

3、提供网闸服务：基于HTTPS安全协议的管理方式；支持SYSLOG协议；支持SNMPX协议；对应用服务器进行设备认证，并对数据格式和内容检查；支持TCP/IP方式传输数据；文件同步功能，支持文件的同步，多级目录结构同步，可进行文件过滤；FTP同步方式，可支持30GB大文件传输；数据库同步，支持触发器、全表、删除原表数据、时序等同步方式；背板带宽不低于4Gbps，TCP/IP实际传输速率不低于800Mbps；数据库同步每秒不低于4000条；文件摆渡方式每秒不低于80Mbps。

4、提供视频隔离服务：交换带宽不低于10Gbps；支持同时在线连接数不低于5万个，万兆光口不低于4个，要求满配光模块，内存不低于32GB；实现内外网安全隔离，保证在隔离条件下的安全数据摆渡；支持数据库、文件、视频流媒体、其他常见TCP/UDP协议数据传输通信，数量不低于8套，支持面向第三方实时提供服务日志，提供配置及策略下发端口。

5、提供前置服务：支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；最大数据文件不低于30GB，并发连接数不低于2万条。

6、提供后置服务：支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；最大数据文件不低于 30GB，并发连接数不低于 2 万条。

7、提供分局到视频专网的隔离服务，每个分局及交管总队不低于 2 套千兆视频边界设备，每套设备要求不低于 200 路视频的并发。

8、提供视频运维管理服务，要求：

数据处理能力不低于 500000 条/分；

交换日志数据查询耗时不超过 3 秒；

数据统计耗时不超过 3 秒；

接口并发能力：300；

无故障运行时间：7×24 小时。

支持首页安全分析大屏、业务分析、运行分析、预警分析、安全模型、资产管理、报表管理、日志审计、上报管理、基础监控、资产画像。

#### 2.3.9.9 联网服务区联网控制服务需求

联网服务区联网控制服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最低满足以下资源要求：

##### 2.3.9.9.1 提供边界网络防护服务

1)提供区分局及交管总队边界网络防护服务：网络层吞吐量不低于 36Gbps，应用层吞吐量数据的安全防护能力不低于 16Gbps，并发连接数不低于 420 万个，新建连接数不低于 30 万次/秒，不少于 4 个千兆电口，不少于 4 个千兆光口，不少于 4 个万兆光口，并要求满配光模块；要求在三年内持续更新对最新威胁的防护能力，需提供可基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组等方式的访问控制能力，具备长连接功能并可以配置连接时长；需提供支持模拟策略匹配的访问控制规则，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，以具备快速排查故障的能力；支持自动生成综合安全风险报表；支持与网络审计服务实现认证联动的能力；支持与终端检测响应服务实现联动；要求设备冗余，支持开放网络数据和防护接口服务，支持第三方调用。

2)提供区分局至下辖派出所边界网络防护服务：网络层吞吐量不低于 20Gbps，应用层吞吐量数据的安全防护能力不低于 18Gbps，并发连接数不低于 800 万个，新建连接数不低于 16 万次/秒，不少于 8 个千兆电口，不少于 6 个万兆光口，并要求满配光模块；要求在三年内持续更新对最新威胁的防护能力，需提供可基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组等方式的访问控制能力，具备长连接功能并可以配置连接时长;需提供支持模拟策略匹配的访问控制规则,输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，以具备快速排查故障的能力；支持自动生成综合安全风险报表；支持与网络审计服务实现认证联动的能力；支持与终端检测响应服务实现联动；要求设备冗余，支持开放网络数据和防护接口服务，支持第三方调用，数量不少于 19 台。

3)提供分局及交管总队联网服务区环网防火墙服务，要求网络层吞吐量不低于 20Gbps，应用层吞吐量不低于 9Gbps，并发连接数不低于 200 万，HTTP 新建连接数不低于 9 万，数量不少于 19 台，单台配置万兆光口不少于 6 个，千兆光口不少于 8 个，要求满配光模块。

4)提供汇聚交换服务,要求交换容量不低于 206Tbps,要求包转发不低于 38400Mpps，单台设备的主控、电源要求冗余，万兆光口数量不低于 48 个，万兆单模光模块满配，千兆光口数量不低于 48 个，千兆多单模光模块满配，千兆电口不低于 48 个，要求设备冗余。汇聚节点需要在 808 机房提供服务。

5)提供到公安部二类系统边界防护服务，网络层吞吐量不低于 18Gbps，应用层吞吐量数据的安全防护能力不低于 8Gbps，并发连接数不低于 400 万个，新建连接数不低于 30 万次/秒，不少于 6 个千兆电口，不少于 4 个千兆光口，不少于 4 个万兆光口，并要求满配光模块；要求在三年内持续更新对最新威胁的防护能力，需提供可基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组等方式的访问控制能力,具备长连接功能并可以配置连接时长;需提供支持模拟策略匹配的访问控制规则，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，以具备快速排查故障的能力；支持自动生成综合安全风险报表；支持与网络审计服务实现认证联动的能力；支持与终端检测响应服务实现联动；要求设备冗余，支持开放网络数据和防护接口服务，支持第三方调用。

#### 2.3.9.9.2 提供数据交换服务

1.提供前置服务：支持基于主流数据库的单、双向数据交换；无需修改数据库表结

构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 1024 张，单表数据影射最大字段数不低于 256 个，数据库到数据库交换记录数不低于 6000 条/秒，最大数据文件不低于 30GB，并发客户端数量不低于 5000 个；支持网络带宽不低于 1Gbps,提供不少于 8 套前置服务。

2.提供后置服务：支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 1024 张，单表数据影射最大字段数不低于 256 个，数据库到数据库交换记录数不低于 6000 条/秒，最大数据文件不低于 30GB，并发客户端数量不低于 5000 个；支持网络带宽不低于 1Gbps,提供不少于 8 套后置服务。

**2.3.9.9.3 提供文件交换服务**

1.提供前置服务：支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 4096 张，单表数据影射最大字段数不低于 256 个，最大数据文件不低于 40GB，并发客户端数量不低于 30000 个；支持网络带宽不低于 10Gbps，提供不少于 2 套前置服务。

2.提供后置服务：支持基于主流数据库的单、双向数据交换；无需修改数据库表结构，不涉及代码修改；可同时发送和接收多个数据库中多个表；支持多种增量方式；可分别定义增加、删除、修改的数据传输；支持时序同步；根据指定字段值进行条件传输；支持大字段数据同步交换；支持异构数据库安全传输；数据传输高度可靠，采用文件落地缓存确认机制进行保证；支持多种文件传输方式；数据库到数据库交换最大并发数据表不低于 4096 张，单表数据影射最大字段数不低于 256 个，数据库到数据库交换记录

数不低于 6000 条/秒，最大数据文件不低于 40GB，并发客户端数量不低于 30000 个；支持网络带宽不低于 10Gbps，提供不少于 2 套后置服务。

#### 2.3.9.10 联网服务区可信服务需求

提供符合公安部要求的可信计算服务，包含且不限于可信报告管理、可信度量管理、可信证书生成、应用签名等功能。

支持与公安部平台的可信管理中心级联并实时上报，满足公安部及本级终端操作系统的可信监测、安全基线认证告警等服务要求。

按照 GA/T 2001 及 GA/T 1466 相关标准要求，提供符合标准规范的数据和相关数据服务接口。

统一管理、三权分立、终端状态监控、审计管理、恶意代码主动防御、可信程序列表、可信动态度量、自主访问控制、强制访问控制、注册表强制访问控制（Windows）、外设控制、软件防卸载、自我保护机制；单节点。

密码服务要求：

对一类应用重要数据进行存储加解密服务，同时对一类应用重要数据提供传输加解密服务，保证数据机密性、完整性和有效性。设备提供标准 SDK 及开发包为一类应用数据提供加解密服务

设备支持 4 个高速加密卡，支持 SM1/SM2/SM3/SM4 国密算法，支持 AES/3DES/RSA/SHA1|256 等国际密码算法；

SM1 加解密：4.6Gbps；SM4 加解密：8Gbps。

#### 2.3.9.11 公安网区安全服务需求

##### 2.3.9.11.1 PKI 认证服务

三类区提供 PKI 认证服务，与现有公安信息网 CA 系统对接，为移动终端、移动应用 APP 提供 CA 认证服务。

##### 2.3.9.11.2 提供堡垒机服务

三类区提供堡垒机服务，含 200 个运维资源授权（可扩展到 1000 个），支持图形协议并发运维数 300 个，支持字符协议并发运维数 1500 个。可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。

##### 2.3.9.11.3 提供到公安网的边界

公安网边界服务根据实际资源使用情况提供弹性资源服务能力，根据当前评估，最

低满足以下资源要求：

1.三类管控区到公安网的边界，服务能力要求：三层吞吐量不低于18Gbps，应用层吞吐量不低于8Gbps；并发连接数不低于400万，新建连接数不低于30万；符合等保2.0二级要求并且满足冗余。

2.提供日志审计服务，要求包含主机审计许可证书数量不低于450，数据盘不低于4TB×2（raid1），平均每秒处理日志数（eps）最大性能不低于3500。内存不低于32GB，硬盘容量不低于128GB minisata+4TB SATA×2，单电源，接口不少于6个千兆电口+2个万兆光口SFP+。

日志分析管理系统是一个专注于信息安全事件的管理平台，该系统提供了安全日志的集中采集、分析挖掘、合规审计、实时监控、日志二次转发及安全告警等功能，能够有效支持审计合规需求和实际运维分析需求，及时发现异常和违规事件，是日常信息安全工作的重要支撑平台。

3.数据库审计服务，最大硬件吞吐量不低于5Gbps，最大数据库纯SQL流量不低于800Mb/s，数据库实例个数：无限制，SQL处理性能不低于50000条SQL/s，日志检索性能不低于1200000条/秒。

内存不低于16GB，硬盘容量不低于128GB SSD+4TB SATA，冗余电源，不低于6个千兆电口。

数据库安全审计系统基于深度数据库协议解析技术，采用自动学习和智能分析模式，实现对数据库访问行为的全程监控、高危操作的实时告警和安全事件的审计追溯。帮助提升数据库访问行为的透明度，降低人工审计成本，真正实现数据库全业务运行可视化、日常操作可监控、危险操作可控制、访问行为可审计、安全事件可追溯。

#### 2.3.9.11.4 符合等保2.0二级要求并且满足冗余

符合等保2.0二级要求并且满足冗余。

### 2.3.10 合规性检测服务需求

#### 2.3.10.1 移动警务等保2.0检测服务需求

根据2016年移动警务总体建设技术方案以及全国公安移动警务升级改造建设任务书要求，Ⅱ类区（市局平台）、Ⅲ类区的建设，从软件、数据、网络、服务器资源、安全、边界等方面的建设需满足最新等保2.0等保三级的要求以及公安部移动警务的特殊安全规定，每年由具备等保测评相关资质单位提供一次等保检测服务并出具等级测评报告；Ⅰ类区、Ⅱ类区（分局和派出所）的建设，从软件、数据、网络、服务器资源、安

全、边界等方面的建设需满足最新等保 2.0 等保二级的要求以及公安部移动警务的特殊安全规定，每两年由具备等保测评相关资质单位提供一次等保检测服务并出具等级测评报告。

#### 2.3.10.2 密评服务需求

根据 2016 年移动警务总体建设技术方案以及全国公安移动警务升级改造建设任务书要求，信息系统建设都需满足密码安全保护测评服务要求以及公安部移动警务的特殊安全规定。Ⅱ类区（市局平台）、Ⅲ类区的建设，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面《信息安全技术信息系统密码应用基本要求》最新版的第三级别要求。由具备密码测评相关资质单位每年提供一次密码合规性测评服务并出具安全性评估报告。

#### 2.3.10.3 安全检测与验收服务需求

提供由公安部部属检测机构提供的软件运行合规性评测服务以及相关报告。成交供应商所提供各项服务需经过功能性能测试验证后方可上线运行，未经北京市公安局主管业务部门确认不得开展移动警务终端入网注册工作。

## 三 其他服务

### 3.1 移动警务整体支撑服务要求

北京市公安局肩负着首都重要的安全保障工作，移动警务是日常工作及重大重要活动期间的基础支撑，具有非常重要的作用。为了确保采购人正常工作的开展，移动警务工作正常运行的支撑服务总体需求：

单警应用支撑服务和移动警务基础设施服务、移动警务安全服务、移动警务应用支撑服务及通用应用服务、交管总队专业应用服务，包括但不限于终端维修、终端信息变更。

#### 3.1.1 日常支撑服务要求

提供移动警务开户、SIM 开通、空中发证、单警应用支撑使用服务的激活、开通、安装、下发等开通注册服务；

提供移动警务开通后的数据搜集、整理、存档后，上交市局相关负责人员；信息应包括 IMSI、ICCID、用户姓名、终端号码、归属地等项；

提供各业务警种应用的开发、上线、开通、下发及相关技术支持；

提供甲方指定的单警应用支撑使用服务的安全管控适配服务；

负责移动警务维护、技术支撑、故障处理、服务升级等相关驻场服务；

负责单警应用支撑使用服务、移动警务应用的故障处理；

提供移动警务业务运维报告，包含：周报、月报、年报、故障处理情况等服务；提供单警应用支撑使用服务、核心设备的备品备件；

提供移动警务对无线网络信号覆盖优化等业务需求；

对采购人的新的业务需求，提供必要的技术支持。

为交管总队单独提供运维值守服务和原厂驻场软件开发及维护服务，负责移动警务维护、版本升级、疑难问题处理、状态监测、故障解决，技术协调、热线服务等。

### 3.1.2 重大重要节庆假日期间的支撑服务要求

提供可行的应急保障服务，包括但不限于：各类设备备件、系统备份、带宽等，确保半小时内恢复故障；

提供 7×24 小时应急移动警务专用 SIM/UIM 卡服务，为甲方用户办理补卡、换卡、查帐、交费等事宜提供方便；

提供 7×24 小时上门服务，负责单警应用支撑使用服务、移动警务应用的故障处理；市区 1 小时到达，郊区 2 小时到达；

提供重大重要事件期间临时性的网络扩容需求；

每日提供移动警务业务运维报告，以及当日故障处理报告；每日根据业务运维情况提出系统运行风险，提前制定应对及解决方案。

### 3.1.3 终端使用支撑服务要求

在终端使用服务期内，发生非人为故障时，提供上门取机服务，提供终端品牌官方授权客户服务中心的 100%原装原厂零件配件的保修服务。在正常使用过程中因意外坠落、碰撞、挤压，造成屏幕、后盖破碎或者开裂时，提供至少每年一次终端品牌官方授权客户服务中心的 100%原装原厂屏幕组件的更换服务，涉及到的相关费用由供应商承担。

### 3.1.4 运营开发服务要求

包括平台软件服务的更新迭代，新服务模块的开发，要求原厂提供开发服务。

定制开发需在市局指定场地现场进行支撑，市局参与移动警务服务过程的管理和人员的考核。并每年对研发过程和研发成果进行考核，根据考核结果对研发团队进行动态调整。

## 3.2 移动警务租用服务时限要求

首批启用移动警务套餐以采购人实际通知为准，成交供应商应当按时将服务涉及的设备运到采购人指定地点，终端设备于合同签订后 20 日内交付；成交供应商提供移动

警务服务所涉及的其他软硬件应当不迟于合同签订后一个月内完成安装、调试。

### 3.3 团队人员

#### 3.3.1 驻场运维岗：

提供日常支撑服务。在采购人指定地点提供 7 个驻场运维岗，全年 365 天 7×24 小时驻场服务；另在交管总队单独设立 1 个驻场运维岗，提供全年 365 天 7×24 小时运维值守服务；

#### 3.3.2 原厂驻场软件开发及维护岗：

（1）在采购人指定地点提供每班不少于 25 人的 5×8 小时的原厂驻场软件开发及维护服务（重大、重要节庆假日期间提升至 7×24 小时的驻场服务维护）。服务人员要求如下：

| 服务内容 | 人员数量 | 备注 |
|---|---|---|
| 泛终端智能协同服务 | 2 | 原厂服务 |
| 统一门户服务 | 2 | 原厂服务 |
| 资源管理服务 | 4 | 包括服务总线和移动服务总线原厂服务 |
| 动态人脸识别 | 1 | 原厂服务 |
| LBS 定位服务 | 1 | 原厂服务 |
| 移动音视频服务 | 3 | 原厂服务 |
| 数据资源开发服务 | 5 | 原厂服务 |
| 证书管理与认证 | 2 | 原厂服务 |
| 移动警务统一运维系统 | 5 | 原厂服务 |

（2）另在交管总队提供每班不少于 4 人的 5×8 小时的原厂驻场软件开发及维护服务（重大、重要节庆假日期间提升至 7×24 小时的驻场服务维护），人员构成应包括项目经理、DBA（OCP 及 OCA）、前端开发人员、后端开发人员。主要负责应用日常维护，并根据业务需求及时对应用进行优化调整。

#### 3.3.3 日常运维岗：

提供日常运维岗，提供不少于 10 人的日常 5×8 上门维护服务。市区 2 小时到达，郊区 4 小时到达。

#### 3.3.4 应急保障岗：

在重大重要节庆假日期间，在采购人指定地点另外提供应急保障岗 1 个，提供 7×24 小时驻场运维服务。

## 四 整体服务设计要求

供应商除提供对应的服务能力，还需按照公安部移动警务技术规范，结合采购人移动警务业务需求，提供符合规范和业务需求的整体服务方案，包含且不仅限于以下内容：

### 4.1 提供北京市公安局移动警务泛物联终端接入和管理设计方案

方案包含但不限于以下内容：

（1）提供泛物联终端直连、桥接型接入认证、访问控制和数据服务标准化的技术实现方案，要求方案包含数据流转图，且符合公安行业规范与移动警务业务需求。

（2）提供云端与边缘端对泛物联终端的管控技术实现方案，要求方案包含业务架构图，合理覆盖各类终端（移动警务终端、智能传感设备、移动执法终端等）管控项及技术手段。

（3）提供泛终端智能协同整体技术架构和方案，要求方案包含云边端服务设计、数据流转图，且完全符合公安行业规范与移动警务安全入网需求。

（4）提供泛物联终端接入管理功能模块详细介绍。

### 4.2 提供北京市公安局移动警务音视频平台整体设计方案

方案包含但不限于以下内容：

（1）提供移动警务音视频采集、传输、存储、分发全流程技术方案，要求方案包含业务架构图，覆盖图传互动、视频调阅、远程会商等场景，符合公安音视频技术规范。

（2）提供音视频平台与现有公安视频系统、指挥调度系统对接方案，要求方案包含逻辑架构图，明确对接标准、数据格式及安全管控措施。

（3）提供音视频平台核心功能模块详细说明。

### 4.3 提供北京市公安局AI助手技术方案和标准化接入方案

方案包含但不限于以下内容：

（1）提供移动警务 AI 助手核心技术方案，包含且不仅限于含语音交互、智能检索、业务辅助、安全防护等，要求方案包含业务架构图，符合公安数据安全规范与移动警务轻量化应用需求。

（2）提供 AI 助手标准化接入技术方案，要求方案包含数据流转图，明确接入协议、接口规范、适配标准，支持与移动警务平台、公安业务系统无缝对接。

（3）提供 AI 助手技术模块功能详细说明。

**4.4 提供北京市公安局移动端门户设计方案（包括认证、应用形态、流程等）**

方案包含但不限于以下内容：

（1）提供移动端统一门户整体架构设计方案，要求方案包含业务架构图，整合移动警务各类应用形态技术方案，符合公安移动应用建设规范。

（2）提供新门户统一身份认证方案（含多因子认证、权限分级、安全审计），要求方案包含逻辑架构图，认证流程、权限控制逻辑，符合公安身份安全管理规范，保障门户访问安全。

（3）提供门户应用形态设计（含元服务、卡片、多媒体消息等）与门户自定义的技术方案，要求方案包含业务示例、数据流转、自定义技术方案、与第三方移动警务平台和应用的对接关系等逻辑。

（4）提供移动端统一门户核心功能详细说明。

**4.5 提供北京市公安局移动警务业务应用迁移过程保障业务连续性的支撑设计方案**

方案包含但不限于以下内容：

（1）提供移动警务业务应用现状分析方案，要求方案包含逻辑架构图、现状痛点及迁移需求分析，贴合移动警务实际业务运行情况。

（2）提供应用迁移网络部署与安全隔离方案，要求方案包含网络部署图，符合公安移动警务网络安全规范，保障迁移过程数据安全与网络稳定。

（3）提供迁移过程业务连续性保障方案，要求包含风险评估、分阶段迁移计划、资源配置、应急处置与回退机制，确保迁移期间业务无中断、数据无丢失。

**4.6 提供北京市公安局泛终端接入开发者管理和技术支撑方案**

方案包含但不限于以下内容：

（1）提供泛终端接入开发者全生命周期管理方案，要求包含清晰的管理流程图（涵盖开发者注册、产品注册、认证、产品上架、审批等环节）。

（2）提供与泛终端智能协同云服务管理平台的技术对接方案，明确对接关系，对接形式（如 REST API、消息队列、数据同步）、数据依赖关系。

（3）提供终端开发者管理核心功能详细说明。

**五 其他要求**

**★供应商需提供相关证明材料，证明其所提供移动警务终端满足北斗独立定位功能，**

材料可为第三方检测机构出具的检测报告复印件或官网截图。

★供应商需提供移动警务终端经过公安部安全与警用电子产品质量检测中心的过检检测报告复印件。

# 第五章　合同草案条款

## 北京市公安局2026年购买移动警务服务项目商务合同

**甲　　方：　北京市公安局**

法定代表人：

地　　址：　北京市东城区前门东大街9号

**乙　　方：**

法定代表人：

地　　址：

乙方在项目编号为_____的“_____”中被确定为成交供应商。双方同意按下述条款和条件签署本合同.

**一、定义**

本合同中的下列术语应解释为：

1. “合同”系指甲乙双方签署的,合同格式中载明双方所达成的协议,包括构成合同的所有的附件、附录和构成合同的所有文件。

2.“合同价”系指根据合同规定,在乙方正确、完全履行合同义务后，甲方应付的价格。

3.“服务”系指根据合同规定乙方承担的相关服务。

**二、合同组成：**

本合同协议书

磋商文件

响应文件

成交通知书

**三、移动警务服务购置明细表**

| 序号 | | 终端 | | 套餐单价 | 启用日期 | 数量 | 服务期内总价（元） |
|---|---|---|---|---|---|---|---|
| | 合约期 | 品牌 | 型号 | （元/月/台） | （年/月/日） | | |
| | | | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

**四、合同金额及支付**

1、合同金额：

人民币（大写）：XXX 元整；人民币（小写）：￥XXXX 元（36 个月）

2、支付方式：

本合同项下移动警务套餐共分 X 批启用，每批次移动警务套餐单独开展资金支付。

(1)第一批（首批）启用日期以套餐开通确认单日期为准，套餐数量 XX 份，合约期 36 个月。

合同签订后，支付 3 个月的服务费￥XX 元；

首批终端设备到货且合同项下全部服务内容通过甲方验收后，乙方向甲方提供合同总金额 5%的履约保函，甲方支付 3 个月服务费￥XX 元。

服务期满一年后，7 个工作日内甲方支付乙方 12 个月服务费￥XX 元。

服务期满两年后，7 个工作日内甲方支付乙方 12 个月服务费￥XX 元。

服务期满三年后，7 个工作日内甲方支付乙方 6 个月服务费￥XX 元。

(2)第二批启用日期以套餐开通确认单日期为准，套餐数量 XX 份，合约期 36 个月

第二批终端设备到货且合同项下全部服务内容通过甲方验收及套餐启用后 7 个工作日内，甲方支付 6 个月服务费￥XX 元。

服务期满一年后，7 个工作日内支付 12 个月服务费￥XX 元。

服务期满两年后，7 个工作日内支付 12 个月服务费￥XX 元。

服务期满三年后，7 个工作日内支付 6 个月服务费￥XX 元。

3、因项目经费拨付原因造成支付延误的，甲方不承担违约责任。

4、甲方每次付款前，乙方需向甲方提供与甲方所付金额相等的正规发票。

**五、交货时间**

首批启用的 XX 份移动警务套餐，乙方应当按时将服务涉及的设备运到甲方指定地点，其中终端设备于合同签订后 20 日内交付；乙方提供移动警务服务所涉及的其他软硬件应当不迟于 2026 年 7 月 31 日完成安装、调试，甲方根据实际情况进行验收。

后续批次启用的 XX 份移动警务套餐，由乙方根据甲方要求将服务涉及的终端设备运到甲方指定地点。

**六、知识产权**

乙方应保证甲方在其本国使用该货物或货物的任何一部分时免受第三方提出的侵犯其专利权、著作权、商标权或工业设计权等知识产权的起诉。如果任何第三方对此提出起诉，乙方应负责与之交涉并承担由此引起的一切法律责任及经济损失。

**七、技术资料**

项目验收合格结束后 3 个工作日内，乙方应将货物中文技术资料一套，如目录索引，图纸，源代码存储介质，技术说明书，操作手册，使用指南，维修指南或服务手册和示意图提交给甲方。如果甲方确认乙方提供的技术资料不完整或在运输过程中丢失，乙方将在收到甲方通知后 3 个日历日内将这些资料提交给甲方。

**八、服务内容**

1.移动警务流量服务

2.移动警务链路服务

3.移动警务增值服务

4.移动警务其他服务

其他内容详见采购及响应文件

**九、履约验收**

1.验收方式：甲方有权按照按下列第_III_种方式对乙方履约情况进行验收，乙方应向甲方提交履约情况报告等作为验收材料，并配合甲方完成履约验收程序。

Ⅰ.一次性验收：乙方服务全部完成，甲方对乙方履约情况进行一次性验收。

Ⅱ.分阶段验收：甲方按照初验、终验对乙方履约情况进行分阶段验收。

Ⅲ.固定周期验收，在终端设备及软件平台完成建设后由北京市公安局进行首次验收，后续甲方根据资金支付节点进行分批次验收。

**九、甲方的权利与义务**

1.选定乙方作为无线数据传输网络运营商，包括但不限于移动警务终端、数据流量、基础管理服务、终端服务、安全保障服务、基础应用服务、TF 加密卡、无线网络覆盖、运维服务等业务和服务。

2.开通该业务的终端号码未经甲方同意，不允许办理过户、销号业务。如遇特殊情况，双方共同协商解决。

3.开通该业务的客户可以享受本协议约定之外的乙方任何涉及本地通话、点对点短信费的优惠或其他任何促销优惠。如遇特殊情况，双方共同协商解决。

4.合同履行期间及服务期结束后，甲方拥有合同项下所有乙方为甲方提供服务所涉

及的软硬件设备的使用权及处置权，甲方在行使上述使用权及处置权时，乙方不得干涉；乙方拥有资产所有权。服务期满后，甲方有权继续无偿使用合同项下所有软硬件，但不得丢弃、出售或转移其他使用途径。如甲方认为需要对合同项下软硬件设备（如警务终端设备）等进行销毁或毁形的，甲方有权自行处置，乙方不得干涉。

5.甲方保证在办理优惠业务时向乙方提供的有关资料真实、有效。如乙方发现上述资料与实际情况不符，乙方有权终止该优惠业务的通信网络服务。

6.若遇资费调整、终端型号更新等，甲方有权要求乙方提高服务标准或服务内容。

7.如遇移动警务终端型号更新或升级，甲方有权无偿获得更新或升级后的终端。

8.如遇乙方通信网络升级，甲方有权在原服务价格不变的情况下，继续享有乙方提供的不间断网络服务。

**十、乙方的权利与义务**

1.乙方有义务为甲方提供本项目相关的咨询建议。

2.在本协议服务期间，乙方提供不间断网络服务。

3.乙方在甲方以后的维护及升级中继续提供业务和技术支持。

4.甲方在本协议期内，如有新业务需求，乙方在 5 个工作日给予答复。

5.乙方提供的优惠业务是针对集团用户定向设计的，用于满足甲方及其员工通信需要。甲方承诺不将优惠业务号卡转让给非甲方员工使用，并承诺不将套餐卡在卡市、零售店、互联网商店等经营场所销售，也不将套餐卡用于通信经营活动中。若违反上述承诺的情况经发现查实，乙方有权取消违规号卡的优惠业务并将甲方违规卡号恢复成乙方一般标准资费。

6.如甲方违反国家对电话客户实名登记的有关规定或乙方的相关规定，包括但不仅限于客户入网实名登记的规范、流程的认真执行、需提供移动电话卡实际使用人的身份证原件、保证人证一致、证件需通过核验、明确使用人与号码一一对应等要求。乙方有权根据本协议，视情节轻重停止提供服务，直至终止协议。

**十一、保密条款**

1.双方承诺，未经对方书面许可，任何一方不得将本协议内容向任何第三方或公众披露、泄漏、散布或公开。

2.在本合同有效期内，双方签署的所有文件或一方提供给另一方的保密资料及保密信息均应遵守国家的相关保密规定及本协议约定，未经对方书面许可，双方均不得向本合同以外的任何第三方或公众披露、泄露、散布或公开。在本合同终止前，由双方共同

商定对这些文件的处理办法。

3 本合作项目中涉及到的双方的任何保密资料、信息将按照国家法律、法规及北京市有关政府规章规定以及双方约定进行管理、合理使用。

4.详细内容见附件保密协议。

**十二、违约责任**

除了本合同第十三条规定的不可抗力事故外，如果乙方不能按合同规定时间准时交货或提供服务，甲方在不影响合同项下的其它补救措施的情况下，可以从合同价款中扣除误期违约金。每延误一天的违约金按迟交货物或未提供服务的服务费用的 0.1%计收。直至交货或提供服务为止。误期违约金的最高限额为合同总价的 10%。

除了本合同第十三条规定的不可抗力事故及合同付款条件约定外，如果甲方不能按合同规定时间准时付款，每延误一日的违约金按迟付费用的 0.1%计收，直至付款为止。误期违约金的最高限额为合同总价的 10%。

如一方有其他违约行为的，应向另一方支付合同总价 10%的违约金。

**十三、不可抗力**

1.本条所述的“不可抗力”系指那些双方在订立合同时无法控制、不可预见的事件。这些事件包括：战争、水灾、地震以及双方同意的事件。当不可抗力事件发生时，执行合同的期限将相应延长。

2.在不可抗力事件发生时，乙方应尽快以书面形式将不可抗力的情况和原因通知甲方。同时必须在 14 个工作日内，以挂号形式递交有关公证机关的证明。如果不可抗力超过 120 个工作日，双方将通过友好协商就合同的执行达成协议。

**十四、争议的解决**

双方在合同有效期内因本合同发生争议，应首先通过友好协商解决；协商不成的，任何一方有权向甲方所在地人民法院提起诉讼。

**十五、违约终止合同**

（一）有下列情形之一的，在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可向乙方发出书面违约通知书，提出终止部分或全部合同。

1.如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部货物或服务；或者乙方提供的货物与服务不能满足合同要求的。

2.如果乙方未能履行合同规定的其它任何义务。

（二）如果甲方根据上述第（一）款的规定，终止了全部或部分合同，甲方可以依

其认为适当的条件和方法购买与未交货物或服务类似的服务，乙方应对购买类似服务所超出的那部分费用负责。但是，乙方应继续执行合同中未终止的部分。

**十六、 转让与分包**

本合同不得转让或分包。

**十七、破产终止合同**

如果乙方破产或无清偿能力，甲方可在任何时候以书面形式通知乙方，终止合同而不给乙方补偿，该终止合同将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权力。

**十八、合同修改**

18.1 任何对合同内容的变更或修改均须双方签订书面的协议书。

**十九、通知**

19.1 本合同任何一方给另一方的通知，都应以书面或电传/传真/电报的方式发送，而另一方应以书面形式确认并发送到对方明确的地址。

**二十、计量单位**

20.1 除技术规范中另有规定外，计量单位均使用国家法定计量单位。

**二十一、适用法律**

21.1 本合同应按照中华人民共和国的法律进行解释。

**二十二、其它事项**

1.本合同其他未尽事宜，待甲乙双方协商签订书面补充协议。

2.任何对合同条件的变更或修改均须双方签订书面的修改书。

3.本合同一式陆份，双方法人或授权代表签字盖章后生效。双方各持叁份，均具有相同的法律效力。下述合同附件为本合同不可分割的部分并与本合同具有同等效力。

**二十三、特别约定**

1.2026 年 7 月 1 日至首批移动警务套餐启用之日期间为过渡期（实际日期以经双方签字盖章的附件 8：套餐开通确认单为准）。

2.过渡期内，乙方负责与原服务商进行协调并向原服务商支付甲方在网用户于过渡期内产生的一切费用，乙方需确保甲方在网用户于过渡期内的业务正常使用。

3.本项目技术合同作为本合同附属文件，内容不同之处以本合同为准。

**二十四、合同附件**

附件 1：移动警务服务终端规格参数及套餐明细

附件 2：增值服务内容

附件 3：增值服务设备清单

附件 4：售后服务方案

附件 5：培训方案

附件 6：实施人员名单

附件 7：保密协议

附件 8：套餐开通确认单

附件 9：网络安全要求

**甲方：北京市公安局**　　**乙方：**

（盖章）　　（盖章）

**甲方代表：**　　**乙方代表：**

**年　　月　　日**　　**年　　月　　日**

**附件 1.移动警务服务终端规格参数及套餐明细**

| 序号 | 合约期 | 终端 | | 月数据流量 | 套餐单价 |
|---|---|---|---|---|---|
| | | 终端品牌 | 终端型号 | 种类 | （元/月/台） |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

移动警务套餐具体内容：

**附件 2.增值服务内容**

（由乙方根据采购文件予以明确）

**附件 3：增值服务设备清单**

| 序号 | 服务项目 | 品名 | 数量 | 品牌 | 型号 | 主要参数 | 备注 |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |

**附件 4.售后服务方案**

1.本项目采购服务内容硬件必须提供到货验收后合约期间免费质量保证；所有软件产品必须提供项目服务期内免费质量保证。提供移动警务终端、核心设备的备品备件；移动终端在服务期内，除人为故意损坏情况外，乙方提供无偿包修包换服务。

2.技术服务包括但不限于提供服务涉及设备的安装、调试、检验、试运行、使用培训、保修、备件备品的购买和软件版本升级等必须的技术支持。提供移动警务开户、SIM 开通、TF 卡制作、移动警务终端的激活、开通、安装、下发等开通注册服务。

3.提供移动警务开通后的数据搜集、整理、存档后，上交市局相关负责人员；信息应包括 IMSI、ICCID、用户姓名、终端号码、归属地等项；提供各业务警种应用的开发、上线、开通、下发及相关技术支持；提供甲方指定的移动警务终端的安全管控适配服务。

4.乙方所投设备制造商在北京市有常设技术支持机构或专业维修队伍和常设备件库。乙方为提供服务涉及设备提供的技术服务均为原厂服务，其中，原厂服务是指技术服务由提供服务涉及设备制造商或其在国内的分支机构直接提供。

5.乙方在服务期内安装的任何零配件，必须是设备生产厂家原产的或是经其认可的，必须是新的未使用和未经修复的，除非最终甲方提供书面许可，否则不可使用此范围外的其他配件或以其它方式替代。服务期内所有因更换或修理货物或部件而导致货物停止运行的时间应从其服务期内扣除。

6.乙方提供 7×24 小时技术响应服务，接到甲方技术支持请求后，必须立即做出实质性响应。对于终端设备故障，必须在 1 小时内恢复设备正常运行，若不能恢复，须提供相同档次的备机。提供日常 7×24 的驻场服务，负责移动警务维护、技术支撑、故障处理、平台升级等相关驻场服务；提供日常提供 5×8 上门服务，负责移动警务终端、移动警务应用的故障处理。

7.团队人员：

（1）驻场运维岗：

提供日常支撑服务。在采购人指定地点提供 7 个驻场运维岗，全年 365 天 7×24 小时驻场服务；另在交管总队单独设立 1 个驻场运维岗，提供全年 365 天 7×24 小时运维值守服务；

（2）原厂驻场软件开发及维护岗：

1）在采购人指定地点提供每班不少于 25 人的 5×8 小时的原厂驻场软件开发及维护服务（重大、重要节庆假日期间提升至 7×24 小时的驻场服务维护）。服务人员要求如下：

| 服务内容 | 人员数量 | 备注 |
| --- | --- | --- |
| 泛终端智能协同服务 | 2 | 原厂服务 |
| 统一门户服务 | 2 | 原厂服务 |
| 资源管理服务 | 4 | 包括服务总线和移动服务总线原厂服务 |
| 动态人脸识别 | 1 | 原厂服务 |
| LBS 定位服务 | 1 | 原厂服务 |
| 移动音视频服务 | 3 | 原厂服务 |
| 数据资源开发服务 | 5 | 原厂服务 |
| 证书管理与认证 | 2 | 原厂服务 |
| 移动警务统一运维系统 | 5 | 原厂服务 |

2）另在交管总队提供每班不少于 4 人的 5×8 小时的原厂驻场软件开发及维护服务（重大、重要节庆假日期间提升至 7×24 小时的驻场服务维护），人员构成应包括项目经理、DBA（OCP 及 OCA）、前端开发人员、后端开发人员。主要负责应用日常维护，并根据业务需求及时对应用进行优化调整。

（3）日常运维岗：提供日常运维岗，提供不少于 10 人的日常 5×8 上门维护服务。市区 2 小时到达，郊区 4 小时到达。

（4）应急保障岗：在重大重要节庆假日期间，在采购人指定地点另外提供应急保障岗 1 个，提供 7×24 小时驻场运维服务。

**附件 5 培训服务方案**

一、培训方式

（一）操作培训

1.培训对象和人数

在警务终端配发过程中，对每个具体使用人员进行操作培训。培训人员包括系统使用人员和终端使用人员。场次与人数无限制。

2.培训时间、地点

培训时间安排：项目实施过程中。

培训地点安排：甲方指定。

3.培训组织

由乙方现场技术人员组织，提供培训材料。

4.培训内容

对用户使用人员进行操作培训，具体包括设备结构、安装步骤、系统切换、应用软件使用方法等

设备操作技术培训；

设备功能、性能、结构介绍；

设备安装、调试、配置培训；

应用软件具体配置；

应用软件具体使用；

日常维护管理知识培训；

简单故障的判断和处理方法；

（二）现场培训

乙方通过现场培训，对用户技术人员讲解产品的结构、安装步骤、调试方法、系统配置、设备维护等。

通过现场培训，保证用户维护人员能对其环境能够有比较全面的了解，将来实际维护中能够熟练地操作。

1.培训对象和人数

在客户现场，配合乙方工程师进行系统安装、配置、调试的相关技术人员和维护人员。场次不少于 3 场，总体培训人数不限。

2.培训时间、地点

培训时间安排：甲方指定时间。

培训地点安排：甲方指定。

3.培训组织

由乙方现场技术人员组织，提供培训材料。

4.培训内容

对用户技术人员进行现场安装调试培训，讲解产品的结构、安装步骤、调试方法、系统配置、设备维护等，现场培训的主要内容包括：

工程实施技术培训；

产品功能、性能、结构介绍；

设备安装、调试、配置培训；

日常维护管理知识培训；

简单故障的判断和处理方法；

（三）系统培训

乙方承诺针对甲方提供系统级培训，包括最新技术、设备操作使用、日常维护以及类似故障的预防和处理经验对甲方提供必要的培训。

1.培训对象

关键用户

设备使用用户

系统维护工程师

系统管理员

管理人员：能够熟练使用本系统进行日常办公和根据权限访问网络资源。

工作人员：能够熟练使用本系统进行日常办公和根据权限访问网络资源。

2.培训方式

为了更好的知识转移，采用设备原厂商及服务提供商对甲方技术人员进行基础操作培训，包括最新技术、设备使用、维护以及运行管理等内容。以现场培训方式为主，场次不少于 3 场，人数不少于 30 人。

3.培训计划

时间安排

| 课程名称 | 适用范围 | 课程时间 | 课程目标 | 备注 |
| --- | --- | --- | --- | --- |
| 系统详细情况介绍 | 全体被培训人员 | 0.5 工作日 | 使得所有用户对基础操作、专用管理平台系统的功能、使用方法、工作方式等有初步了解 | 人工授课方式 |
| 最终用户培训 | 客户端软件使用人员（或代表） | 0.5 工作日 | 使得业务最终使用人员对于终端软件的详细功能和使用方法能熟练掌握,能进行基本的故障定位与排除。 | 人工授课方式、模拟演练 |
| 管理人员培训 | 市局系统管理人员 | 1.5 工作日 | 使市局系统管理人员能理解整套系统的运行方式与工作流程，了解客户端的功能及使用，能进行基本的故障定位与排除。 | 人工授课方式、模拟演练 |
| 效果考核及总结 | 全体被培训人员 | 0.5 工作日 | 通过笔试，上机测试等方式对被培训者的学习情况进行考核并进行记录和反馈 | |

4.培训地点

地点由用户安排，需要有培训所需的环境。

5.培训内容

（1）系统管理和维护培训

通过培训，用户可以掌握管理信息系统的部署和运行、用户管理、软件升级管理、数据备份/数据恢复。系统管理员为软件操作人员提供帮助,培训对象为本系统的系统管理员。

（2）软件操作人员培训

以用户手册为基础，培训软件应用操作人员如何使用管理信息系统，培训对象为软件操作人员：

－管理信息系统使用（连接、密码、录入）和界面操作

－管理信息系统的管理

－信息数据规范和录入操作规范

（3）网络管理人员培训

在项目的进行过程中始终和用户保持密切的联系，从而保证用户对整个系统的技术

进展有一个详细的了解。在项目进行的同时，我们还将对用户作出以下方面的现场培训，使用户在工程结束后可以马上管理、使用好该系统，迅速的使系统投入正常的运做中并且充分发挥效益。

**附件 6：实施人员名单**

（由乙方根据实际参与项目人员补充）

**附件 7：保密协议**

# 保密协议

为确保本合同建设的秘密安全，根据公安部、国家保密局关于《公安工作国家秘密范围的规定》（公通字（2019）3 号）、《公安机关警务工作秘密范围的规定》（公通字（2019）2 号）文件规定，凡涉及秘密范围的项目建设，双方就

_____保密事宜达成如下一致意见：

1、本合同所涉及的项目，涉及公安工作秘密，乙方承诺本公司以及乙方所有参与项目建设的工作人员，均遵守本协议对该项目的各种资料和信息予以保密。

2、乙方有责任在投标（谈判）及合同履行中，对甲方提供的全部信息数据、文件资料等进行保密，乙方不得在任何时间、任何场合向第三方泄露。

3、乙方应保证参加项目建设的单位资质、人员、技术、设备符合甲方的要求，未经甲方许可，不得更换。

4、未经甲方许可，乙方不得将其承担的项目转让给第三方或与第三方共同开发。

5、乙方对甲方提供的与项目有关的技术资料、秘密文件不得丢失，不得自行复制，不得向第三人提供，项目完成后应马上归还甲方。

6、项目实施期间，乙方应掌握其工作人员资质、自然情况，对参见项目实施的工作人员登记造册，并就其工作人员的保密义务责任承担法律上的担保责任。保证发生泄密情况后，能为甲方提供查找相关的工作人员和泄密原因的线索和证据，并承担相应责任。

7、因乙方原因泄密的，甲方有权随时解除主合同，乙方须无条件退还已经收到的甲方已付款，并向甲方支付主合同总价 10%的违约金；对因泄密所造成的后果，乙方还应当承担相应的法律责任（包括并不限于承担赔偿责任等）。

8、本协议为主合同不可分割的组成部分，为主合同的有效补充。本协议一式 陆 份，双方各执 叁 份，自双方签字盖章之日起生效。

**甲方（签字盖章）：** **乙方（签字盖章）：**

日期：　　年　　月　　日　　日期：　　年　　月　　日

# 北京市公安局2026年购买移动警务服务项目

## 开通确认单

<table>
<tr><td>甲方单位名称</td><td colspan="3"></td></tr>
<tr><td>乙方单位名称</td><td colspan="3"></td></tr>
<tr><td>服务开通日期<br>（年/月/日）</td><td colspan="3"></td></tr>
<tr><td>服务期限</td><td colspan="3">服务期限为36个月<br>自　　年　　月　　日至　　年　　月　　日</td></tr>
<tr><td>移动终端型号</td><td></td><td>本次开通数量</td><td></td></tr>
<tr><td>甲方项目联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>乙方项目联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td colspan="4">根据《北京市公安局2026年购买移动警务服务项目商务合同》合同编号_____约定，乙方单位于_____年_____月_____日开通共计_____部套餐服务并全部交付于甲方，经甲方确认与本次乙方提供的套餐服务与合同约定内容一致，予以签收。</td></tr>
<tr><td colspan="4">自合同生效之日起至本确认单签署之日止，乙方已为甲方开通共计_____部套餐服务（含本次开通数量），剩余共计_____部套餐未开通。</td></tr>
<tr><td colspan="4">其它有关告知事项（备注）：</td></tr>
<tr><td colspan="2">客户签收负责人签字：<br>电话：<br>（单位盖章）</td><td colspan="2">XX公司客户经理签字：<br>电话：<br>（单位盖章）</td></tr>
<tr><td colspan="2">年　　月　　日</td><td colspan="2">年　　月　　日</td></tr>
</table>

附件 9：

# 网络安全要求

## 一、基本安全要求

1.1 乙方供应的产品应当符合有关法律、行政法规、强制性国家标准；若乙方提供的产品为网络关键设备和网络安全专用产品，则应当按照《中华人民共和国网络安全法》及相关国家标准的强制性要求，产品经过相关检测与认证；涉及密码产品的应符合《中华人民共和国密码法》的要求。

1.2 乙方提供的产品中不得设置恶意程序，不得故意留有后门、木马等程序和功能。

1.3 乙方不得在产品中设置隐蔽接口，不得加载能够禁用或绕过安全机制的组件，不得非法远程控制甲方产品。

1.4 乙方不得根据国外法律向境外机构提供与本项目相关的信息，如项目信息、甲方信息、项目材料、相关数据等，或为其获取相关信息提供便利条件。

1.5 乙方未经甲方书面授权，不得将甲方数据用于与本项目无关的系统演示、测试、开发等场景。

1.6 乙方应配合甲方开展供应链安全监督和检查工作，应保证供应链上传递的供应信息的真实性、准确性、完整性，并采取措施保护信息不被篡改和泄露。

1.7 乙方应提供满足本项目产品持续稳定运行所需的产品使用授权，包括但不限于许可证、产品授权序列号等。

1.8 乙方应配合甲方对其开展的远程检测和现场检查。

## 二、交付安全要求

2.1 乙方应保障产品在物流环节的完整性、网络传输过程中的完整性和机密性，防止数据泄露、恶意篡改和损毁等事件发生。

2.2 乙方应确保供应的产品不存在已知漏洞未处置或已公开漏洞未修复的情况；对于存在已公开漏洞未修复的，应当立即采取补救措施，按照规定及时告知甲方并按照相关规定向有关主管部门报告，涉及危害国家安全、公共利益的，应协助甲方在 24 小时内履行报告义务。

2.3 乙方应为产品提供开源组件清单、合格证、产品认证证书（如 CCC 产品认证证书、网络安全专用产品安全检测证书）等相关文件。

2.4 乙方应提供产品相关技术资料，包括但不限于中文版运行维护、使用说明书等技术资料。

2.5 乙方应向甲方明示包含在产品中的所有功能模块、外部接口，告知甲方系统中预

置的所有账户和默认口令，甲方应立即进行修改。

2.6 乙方应配合甲方制定网络安全事件应急预案，主动配合甲方采取消除安全隐患的措施，防止危害扩大。

2.7 甲乙双方应在产品进行升级维护时，采用安全可控的渠道交付升级包、补丁包，并开展相应的安全性测试、完整性校验等工作。

2.8 甲方拥有对乙方提供的产品安装和升级等的知情权和选择权，乙方在安装和升级时明示甲方并获得同意后方可进行操作。

**三、替换与废止安全要求**

3.1 乙方不得通过技术手段限制甲方选择其他供应商的产品、组件或技术。

3.2 乙方应为甲方数据和业务在不同产品间的迁移提供必要的技术支持。

3.3 甲方产品停止使用时乙方应提供必要的技术支持，协助甲方进行数据迁移或数据导出。

3.4 乙方应在发生组织架构重大调整（如重组、收购、外资控股等）或服务外包时，及时通知甲方并采取措施保证甲方相关信息的安全。

3.5 乙方针对本项目中使用的产品或外部组件，不再维护而退市时，应提前发布退市公告，并通知甲方。

**四、安全漏洞管理要求**

4.1 乙方应建立和执行针对本项目产品的安全漏洞的应急响应机制和流程，对发现的产品安全漏洞采取修复或缓解措施，及时告知甲方安全风险和可用的补救措施，并按规定向有关主管部门报告。

4.2 乙方应当为交付的产品提供安全维护，在规定或约定的期限内，不得终止安全维护；针对本项目产品乙方不得因产品维护到期、过质保期、产品退市等任何理由停止安全维护。本项目产品出现实际可利用的高危及以上等级漏洞时，乙方仍应为甲方提供有偿的安全维护服务（具体费用在协议签订时双方协商），在规定或约定的期限内采取措施进行修补或提供缓解方案，为甲方提供漏洞通知和补丁下载服务，并对甲方漏洞修复给予必要的技术支持。乙方应将甲方对其的安全维护要求同步约束至上游供应商。

**五、其他**

5.1 乙方应按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《网络数据安全管理条例》《关键信息基础设施安全保护条例》《商用密码管理条例》等法律法规及规章制度的要求，履行网络和数据安全保护义务。

# 第六章　响应文件格式

**供应商编制文件须知**

1、供应商按照本部分的顺序编制响应文件，编制中涉及格式资料的，应按照本部分提供的内容和格式（所有表格的格式可扩展）填写提交。

2、对于竞争性磋商文件中标记了“实质性格式”文件的，供应商不得改变格式中给定的文字所表达的含义，不得删减格式中的实质性内容，不得自行添加与格式中给定的文字内容相矛盾的内容，不得对应当填写的空格不填写或不实质性响应，**否则响应无效**。未标记“实质性格式”的文件和竞争性磋商文件未提供格式的内容，可由供应商自行编写。

3、全部声明和问题的回答及所附材料必须是真实的、准确的和完整的。

响应文件封面（非实质性格式）

# 响 应 文 件

项目名称：
项目编号：

供应商名称：

1 满足《中华人民共和国政府采购法》第二十二条规定

1-1 营业执照等证明文件

1-2 供应商资格声明书（实质性格式）

# 供应商资格声明书

致：采购人或采购代理机构

在参与本次项目磋商中，我单位承诺：

（一） 具有良好的商业信誉和健全的财务会计制度；

（二） 具有履行合同所必需的设备和专业技术能力；

（三） 有依法缴纳税收和社会保障资金的良好记录；

（四） 参加政府采购活动前三年内，在经营活动中没有重大违法记录（重大违法记录指因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚，不包括因违法经营被禁止在一定期限内参加政府采购活动，但期限已经届满的情形）；

（五） 我单位不属于政府采购法律、行政法规规定的公益一类事业单位、或使用事业编制且由财政拨款保障的群团组织（仅适用于政府购买服务项目）；

（六） 我单位不存在为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务后，再参加该采购项目的其他采购活动的情形（单一来源采购项目除外）；

（七） 与我单位存在“单位负责人为同一人或者存在直接控股、管理关系”的其他法人单位信息如下（如有，不论其是否参加同一合同项下的政府采购活动均须填写，如没有请写“无”）：

| 序号 | 单位名称 | 相互关系 |
|---|---|---|
| 1 | | |
| 2 | | |
| … | | |

上述声明真实有效，否则我方负全部责任。

供应商名称（加盖公章）：_____

日期：____年____月____日

说明：供应商承诺不实的，依据《政府采购法》第七十七条“提供虚假材料谋取中标、成交的”有关规定予以处理。

2 落实政府采购政策需满足的资格要求（如有）

2-1 中小企业政策证明文件**（本项目不专门面向中小企业预留采购份额）**

说明：

（1）如本项目（包）不专门面向中小企业预留采购份额，供应商无须提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件；当供应商拟享受中小企业扶持政策时，仍应提供上述证明文件，否则不享受相关中小企业扶持政策。

（2）如本项目（包）专门面向中小企业采购，响应文件中须提供《中小企业声明函》或《残疾人福利性单位声明函》，或提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（3）如本项目（包）预留部分采购项目预算专门面向中小企业采购，且要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业或要求供应商以联合体形式参加采购活动，响应文件中须提供《中小企业声明函》或《残疾人福利性单位声明函》或由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

（4）中小企业声明函填写注意事项

1）《中小企业声明函》由参加政府采购活动的供应商出具。联合体参与的，《中小企业声明函》可由牵头人出具。

2）对于联合体中由中小企业承担的部分，或者分包给中小企业的部分，必须全部由中小企业制造、承建或者承接。供应商应当在声明函“标的名称”部分标明联合体中中小企业承担的具体内容或者中小企业的具体分包内容。

3）对于多标的采购项目，供应商应充分、准确地了解所提供货物的制造企业、提供服务的承接企业信息。对相关情况了解不清楚的，不建议填报本声明函。

（5）温馨提示：为方便广大中小企业识别企业规模类型，工业和信息化部组织开发了中小企业规模类型自测小程序，在国务院客户端和工业和信息化部网站上均有链接，供应商填写所属的行业和指标数据可自动生成企业规模类型测试结果。本项目中小企业划分标准所属行业详见第二章《供应商须知资料表》，如在该程序中未找到本项目文件规定的中小企业划分标准所属行业，则按照《关于印发中小企业划型标准规定的通知（工信部联企业〔2011〕300号）》及《金融业企业划型标准规定》（银发〔2015〕309 号）等国务院批准的中小企业划分标准执行。

2-1-1 中小企业证明文件

# 中小企业声明函（服务）格式

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加（单位名称）的（项目名称）采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

（标的名称），属于（采购文件中明确的所属行业）行业；承接企业为（企业名称），从业人员_____人，营业收入为_____万元，资产总额为_____万元[1]，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：_____

日 期：_____

[1] 从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

# 中小型企业划分标准

关于印发中小企业划型标准规定的通知工信部联企业〔2011〕300 号

一、根据《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》(国发〔2009〕36 号)，制定本规定。

二、中小企业划分为中型、小型、微型三种类型，具体标准根据企业从业人员、营业收入、资产总额等指标，结合行业特点制定。

三、本规定适用的行业包括：农、林、牧、渔业，工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。

四、各行业划型标准为：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从

业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

**（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企**

**业。**

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

# 残疾人福利性单位声明函格式

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定，本单位**（请进行选择）：**

**□不属于符合条件的残疾人福利性单位。**

**□属于符合条件的残疾人福利性单位，**且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

**本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。**

单位名称（盖章）：_____

日　期：_____

2-1-2 拟分包情况说明及分包意向协议**（本项目不允许分包）**

说明：

如本项目（包）允许分包，且供应商拟进行分包时：

（1）响应文件中须提供《拟分包情况说明》，否则**响应无效**；

（2）当同时符合下列情形时，响应文件还须提供《分包意向协议》，否则**响应无效**：

A. 本项目（包）预留部分采购项目预算专门面向中小企业采购，且要求获得采购合同的供应商将采购项目中的一定比例分包给一家或者多家中小企业的；

B. 供应商通过分包方式满足中小企业政策要求的。

**（3）不属于上述情形时，无须提供《拟分包情况说明》及《分包意向协议》。**

# 拟分包情况说明

致：（采购人或采购代理机构）

我单位参加贵单位组织采购的项目编号为_____的_____项目（填写采购项目名称）中_____包（填写包号）的磋商。拟签订分包合同的单位情况如下表所示，我单位承诺一旦在该项目中获得采购合同将按下表所列情况进行分包，同时承诺分包承担主体不再次分包。

| 序号 | 分包承担主体名称 | 分包承担主体类型（选择） | 资质等级 | 拟分包合同内容 | 拟分包合同金额（人民币元） | 占该采购包**合同金额的**比例（%） |
|---|---|---|---|---|---|---|
| 1 | | □中型企业<br>□小微企业<br>□其他 | | | | |
| 2 | | □中型企业<br>□小微企业<br>□其他 | | | | |
| … | | | | | | |
| | | | | 合计： | | |

供应商名称（加盖公章）：_____

日期：___年___月___日

注：

（1）当供应商属于本部分说明中第（1）类情形，如未提供《拟分包情况说明》，或提供了《拟分包情况说明》但未填写分包承担主体名称、拟分包合同内容、拟分包合同金额，其**响应无效**；

（2）当供应商属于本部分说明中第（2）类情形，如未提供《拟分包情况说明》，或提供了《拟分包情况说明》但未填写分包承担主体名称、分包承担主体类型、拟分包合同内容、拟分包合同金额，其**响应无效**；

（3）如本采购文件《供应商须知资料表》载明本项目分包承担主体应具备的相应资质条件，则供应商须在本表中列明分包承担主体的资质等级，并后附资质证书复印件，否则**响应无效**。

# 分包意向协议

甲方（供应商）：_____

乙方（拟分包单位）：_____

甲方承诺，一旦在_____（采购项目名称）（项目编号/包号为：_____）采购项目中获得采购合同，将按照下述约定将合同项下部分内容分包给乙方：

1.分包内容：_____。

2.分包金额：_____，该金额占该采购包合同金额的比例为_____%。

乙方承诺将在上述情况下与甲方签订分包合同。

本协议自各方盖章之日起生效，如甲方未在该项目（采购包）成交，本协议自动终止。

甲方（盖章）：_____　　乙方（盖章）：_____

日期：_____年_____月_____日

注：

（1）当供应商属于本部分说明中第（2）类情形，必须提供，否则**响应无效**；其他情形无须提供；

（2）供应商须与所有拟分包单位分别签订《分包意向协议》，每单位签订一份，并在响应文件中提交全部协议原件，否则**响应无效**。

2-2 其它落实政府采购政策的资格要求（如有）

提供供应商资格声明书（格式），已提供过的不用重复提供。

3 本项目的特定资格要求（如有）**（本项目不接受联合体）**

3-1 联合协议（如有）

# 联合协议

_____ 、_____及_____就“_____（项目名称）”_____包采购项目的磋商事宜，经各方充分协商一致，达成如下协议：

一、 由_____牵头，_____、_____参加，组成联合体共同进行采购项目的磋商工作。

二、 联合体成交后，联合体各方共同与采购人签订合同，就采购合同约定的事项对采购人承担连带责任。

三、 联合体各方均同意由牵头人代表其他联合体成员单位按竞争性磋商文件要求出具《授权委托书》。

四、 牵头人为项目的总负责单位；组织各参加方进行项目实施工作。

五、 _____负责_____，具体工作范围、内容以响应文件及合同为准。

六、 _____负责_____，具体工作范围、内容以响应文件及合同为准。

七、 _____负责_____（如有），具体工作范围、内容以响应文件及合同为准。

八、 本项目联合协议合同总额为_____元，联合体各成员按照如下比例分摊（按联合体成员分别列明）：

（1）_____为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为_____元；

（2）_____为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为_____元；

（…）_____为□大型企业□中型企业、□小微企业（包含监狱企业、残疾人福利性单位）、□其他，合同金额为_____元。

九、 以联合体形式参加政府采购活动的，联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

十、 其他约定（如有请填写具体内容，如没有请填写“无”）：_____。

本协议自各方盖章后生效，采购合同履行完毕后自动失效。如未成交，本协议自动终止。

联合体牵头人名称：_____　　联合体成员名称：_____

盖章：_____　　盖章：_____

联合体成员名称：_____

盖章：_____

日期：_____年_____月_____日

注：

1. 如本项目（包）接受供应商以联合体形式参加采购活动，且供应商以联合体形式参与时，须提供《联合协议》，否则**响应无效**。非联合体供应商参加本次采购活动的无须提供《联合协议》。
2. 联合体各方成员须在本协议上共同盖章。

3-2 其他特定资格要求：

供应商具备有效的中华人民共和国基础电信业务经营许可证。提供证明文件的复印件并加盖公章。

4 磋商保证金凭证/交款单据复印件

5　响应书（实质性格式）

# 响应书

致：（采购人或采购代理机构）

我方参加你方就_____（项目名称，项目编号）组织的采购活动，并对此项目进行磋商。

1. 我方已详细审查全部竞争性磋商文件，自愿参与磋商并承诺如下：

（1）本响应有效期为自响应文件提交截止之日起_____个日历日。

（2）除合同条款及采购需求偏离表列出的偏离外，我方响应竞争性磋商文件的全部要求。

（3）我方已提供的全部文件资料是真实、准确的，并对此承担一切法律后果。

（4）如我方成交，我方将在法律规定的期限内与你方签订合同，按照竞争性磋商文件要求提交履约保证金，并在合同约定的期限内完成合同规定的全部义务。

2. 其他补充条款（如有请填写具体内容，如没有请填写“无”）：_____。

与本磋商有关的一切正式往来信函请寄：

地址_____　　传　真_____

电话_____　　电子函件_____

供应商名称（加盖公章）：_____

日期：____年____月____日

6　授权委托书（实质性格式）

# 授权委托书

本人____（姓名）系____（供应商名称）的法定代表人（单位负责人），现委托_____（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、提交、撤回、修改____（项目名称）响应文件和处理有关事宜，其法律后果由我方承担。

委托期限：自本授权委托书签署之日起至响应有效期届满之日止。

代理人无转委托权。

供应商名称（加盖公章）：_____

法定代表人（单位负责人）（签字或签章）：_____

委托代理人（签字或签章）：_____

日期：____年____月____日

**附：法定代表人（单位负责人）及委托代理人身份证明文件复印件：**

说明：

1.若供应商为事业单位或其他组织或分支机构，则法定代表人（单位负责人）处的签署人可为单位负责人。

2.若响应文件中签字之处均为法定代表人（单位负责人）本人签署，则可不提供本《授权委托书》，但须提供《法定代表人（单位负责人）身份证明》；否则，不需要提供《法定代表人（单位负责人）身份证明》。

3.供应商为自然人的情形，可不提供本《授权委托书》。

4.供应商应随本《授权委托书》同时提供法定代表人（单位负责人）及委托代理人的有效的身份证或护照等身份证明文件复印件。提供身份证的，应同时提供身份证**双面**复印件。

# 法定代表人（单位负责人）身份证明

致：____（采购人或采购代理机构）

兹证明，

姓名：____性别：____年龄：____职务：____

系_____（供应商名称）的法定代表人（单位负责人）。

**附：法定代表人（单位负责人）身份证或护照等身份证明文件复印件：**

供应商名称（加盖公章）：_____

法定代表人（单位负责人）（签字或签章）：_____

日期：____年____月____日

7　报价一览表

# 报价一览表

项目编号：_____　　项目名称：_____

| 供应商名称 | 报价 | |
|---|---|---|
| | 大写 | 小写 |
| | | |

注：1.此表中，每包的报价应和《分项报价表》中的总价相一致。
　　2.本表必须按包分别填写。

供应商名称（加盖公章）：_____

日期：____年____月____日

8　分项报价表

# 分项报价表

项目编号：_____　　项目名称：_____　　报价单位：人民币元

| 序号 | 分项名称 | 单价（元） | 数量 | 合价（元） | 备注/说明 |
|---|---|---|---|---|---|
| 1 | 移动警务套餐 | | 54817 | | 包含本项目采购需求及合同中的所有服务内容 |
| 总价（元） | | | | | |

注：1.本表应按包分别填写。
2.如果不提供分项报价将视为没有实质性响应招标文件。
3.上述各项的详细规格（如有），可另页描述。

供应商名称（加盖公章）：_____

日期：____年____月____日

9　合同条款偏离表（实质性格式）

# 合同条款偏离表

项目编号：_____　　项目名称：_____

| 序号 | 竞争性磋商文件条目号（页码） | 竞争性磋商文件要求 | 响应文件内容 | 偏离情况 | 说明 |
|---|---|---|---|---|---|
| **对本项目合同条款的偏离情况（**应进行选择，未选择**响应无效）：**<br>**□无偏离**（如无偏离，仅选择无偏离即可；无偏离即为对合同条款中的所有要求，均视作供应商已对之理解和响应。）<br>**□有偏离**（如有偏离，则应在本表中对负偏离项逐一列明，否则响应无效；对合同条款中的所有要求，除本表列明的偏离外，均视作供应商已对之理解和响应。） | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

注：　“偏离情况”列应据实填写“正偏离”或“负偏离”。

供应商名称（加盖公章）：_____

日期：____年____月____日

10　采购需求偏离表（实质性格式）

# 采购需求偏离表

项目编号：_____　　项目名称：_____

| 序号 | 竞争性磋商文件条目号(页码) | 竞争性磋商文件要求 | 响应内容 | 偏离情况 | 说明 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

注：
1. 对竞争性磋商文件中的所有商务、技术要求，除本表所列明的所有偏离外，均视作供应商已对之理解和响应。此表中若无任何文字说明，内容为空白的，**响应无效**。
2.“偏离情况”列应据实填写“无偏离”、“正偏离”或“负偏离”。

供应商名称（加盖公章）：_____

日期：____年____月____日

11 本国产品标准证明文件（**本项目不适用**）

# 关于符合本国产品标准的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，本公司（单位）提供的以下产品属于本国产品。具体情况如下：

1.（产品名称 1）[1]，生产厂为（厂名）[2]，厂址为（生产厂址）。（产品名称 1）的中国境内生产的组件成本占比≥（规定比例）[3]。（产品名称 1）的（关键组件）[4]在中国境内生产。（产品名称 1）的（关键工序）[5]在中国境内完成。

2.（产品名称 2），生产厂为（厂名），厂址为（生产厂址）。（产品名称 2）的中国境内生产的组件成本占比≥（规定比例）。（产品名称 2）的（关键组件）在中国境内生产。（产品名称 2）的（关键工序）在中国境内完成。

……

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：

日期：　　年　　月　　日

注：1.产品如有型号，请在“产品名称”栏一并填写。

2.生产厂名与厂址应与生产厂营业执照载明的相关信息保持一致。

3.该产品的中国境内生产的组件成本占比相关要求实施前，“规定比例”栏可不填。

4.该产品的关键组件要求实施前，“关键组件”栏可不填。

5.该产品的关键工序要求实施前，“关键工序”栏可不填。

# 产品成本占比承诺函

我公司（单位）郑重承诺，我公司已阅读并理解《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定。据此承诺如下：

为本采购项目或者采购包提供的符合本国产品标准的产品成本之和占提供的全部产品成本之和的比例为_____%。

公司（单位）名称（盖章）：

日期：　　年　　月　　日

注：

1. 本承诺函应按包分别提供。

2. 单一产品采购无须提供本承诺函；供应商提供产品全部为本国产品，且提供了《关于符合本国产品标准的声明函》时，无须提供本承诺函。

3. 当采购项目或单个采购包中含有多种产品，且供应商提供的产品同时包含本国产品及非本国产品，则供应商除需提供《关于符合本国产品标准的声明函》外，还需提供本承诺函；否则，不享受价格评审优惠。

12　竞争性磋商文件要求提供或供应商认为应附的其他材料

12-1 供应商信息采集表

| 供应商名称 | 供应商所属性别 | 外商投资类型 |
| --- | --- | --- |
| | | |
| | | |
| | | |
| | | |

注：1.供应商如为联合体，则应填写联合体各成员信息。

2.供应商所属性别请填写“男”或“女”，指拥有供应商 51%以上绝对所有权的性别；绝对所有权拥有者可以是一个人，也可以是多人合计计算。

3.外商投资类型请填写“外商单独投资”、“外商部分投资”或“内资”。

12-2 北京市公安局供应商不良行为记录告知书（实质性格式）

# 北京市公安局供应商不良行为记录告知书

项目名称：_____

企业名称：_____

为加强市公安局项目建设，规范供应商与全局合作行为，现就市公安局供应商不良行为记录管理相关内容进行告知。

与市公安局合作的供应商有下列情形之一的，其具体行为将被列入市公安局供应商不良行为记录：

（一）依据《中华人民共和国政府采购法》第七十七条有以下情形之一的：

1.提供虚假材料谋取中标、成交的；

2.采取不正当手段诋毁、排挤其他供应商的；

3.与采购人、其他供应商或者采购代理机构恶意串通的；

4.向采购人、采购代理机构行贿或者提供其他不正当利益的；

5.在招标采购过程中与采购人进行协商谈判的；

6.拒绝有关部门监督检查或者提供虚假情况的。

（二）依据《中华人民共和国政府采购法实施条例》第七十二条有以下情形之一的：

1.向评标委员会、竞争性谈判小组或者询价小组成员行贿或者提供其他不正当利益；

2.中标或者成交后无正当理由拒不与采购人签订政府采购合同；

3.未按照采购文件确定的事项签订政府采购合同；

4.将政府采购合同转包；

5.提供假冒伪劣产品；

6.擅自变更、中止或者终止政府采购合同。

（三）依据《中华人民共和国政府采购法实施条例》第七十三条，捏造事实、提供虚假材料或者以非法手段取得证明材料进行投诉的。

（四）依据《中华人民共和国政府采购法实施条例》第七十四条有以下情形之一的：

1.供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关情况并修改其投标文件或者响应文件；

2.供应商按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件；

3.供应商之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

4.属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；

5.供应商之间事先约定由某一特定供应商中标、成交；

6.供应商之间商定部分供应商放弃参加政府采购活动或者放弃中标、成交；

7.供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商中标、成交或者排斥其他供应商的其他串通行为。

（五）依据《公务员法》《中国共产党纪律处分条例》《关于规范公务员辞去公职后从业行为的意见》等法律、法规、规定，录用市公安局退休、辞职、辞退、开除不满三年的工作人员，且提供与其原工作直接相关业务的岗位的；

（六）在与市公安局合作过程中，发生失泄密问题、不履行或迟延履行合同义务或存在其他违约行为，且消极推诿、拒绝承担违约责任，被解除合作协议、终止合同履行、启动司法程序的，或造成市公安局利益损失的。

（七）有其他损害市公安局利益行为的，或造成不良影响的。

我单位已知悉上述内容，并自愿承担相关责任。

企业名称：（公章）

法定代表人（单位负责人）：_____（签字或签章）

年　　月　　日

12-3 超流量池部分流量费单价说明

# 超流量池部分流量费单价说明

致：北京市公安局

我单位声明，针对本项目超流量池部分流量费单价为：_____元/G。

投标人名称（加盖公章） _____

日期：_____年_____月_____日

12-4 承诺函

# 承诺函

致：北京市公安局

我单位承诺：

（1）完全满足竞争性磋商文件中第四章 采购需求中“2.1.2 移动警务流量110GB 需求”的“单警应用支撑服务需求”的全部需求内容，无负偏离。

（2）完全满足竞争性磋商文件中第四章 采购需求 “三 其他服务”中“3.2 移动警务租用服务时限要求”的全部内容，无负偏离。

（3）拟派本项目的团队人员完全满足响应竞争性磋商文件中第四章 采购需求“三 其他服务”中“3.3 团队人员”的全部内容，无负偏离。

投标人名称（加盖公章） _____

日期：_____年_____月_____日

14 最后报价一览表（实质性格式，磋商后提交）

# 最后报价一览表

项目编号：0610-2641NF051066

项目名称：市局 2026 年购买移动警务服务项目

| 供应商名称 | 最后报价 | | 其他声明 |
|---|---|---|---|
| | 大写 | 小写 | |
| | | | |

注：1.此表中，每包的最后报价应和《最后分项报价表》中的总价相一致。
2.本表必须按包分别填写。
3.此表无需在响应文件中提交，磋商后供应商按磋商小组要求提交。

供应商授权代表签字（或加盖供应商公章）：_____

日期：____年____月____日

15 最后分项报价表（实质性格式，磋商后提交）

# 最后分项报价表

项目编号：0610-2641NF051066
项目名称：市局 2026 年购买移动警务服务项目
报价单位：人民币元

| 序号 | 分项名称 | 单价（元） | 数量 | 合价（元） | 备注/说明 |
|---|---|---|---|---|---|
| 1 | 移动警务套餐 | | 54817 | | 包含本项目采购需求及合同中的所有服务内容 |
| | | | 总价（元） | | |

注：1.本表应按包分别填写。
2.上述各项的详细规格（如有），可另页描述。
3.此表无需在响应文件中提交，磋商后供应商按磋商小组要求提交。

供应商授权代表签字（或加盖供应商公章）：_____

日期：____年____月____日

## 成交服务费承诺书（格式）

致：北京国际招标有限公司：

我们在贵公司组织的市局 2026 年购买移动警务服务项目竞争性磋商项目中若能成交（磋商文件编号：0610-2641NF051066），我们保证在收到成交通知书后按竞争性磋商文件的规定，以转账支票、电汇、网上银行转账或现金的形式，向贵公司即北京国际招标有限公司（地址：北京市东城区朝内北小街 71 号，开户银行：华夏银行建国门支行，账号：10265000000524102）一次性支付应该交纳的成交服务费用。收费标准按照成交金额依据以下规定的成交代理服务收费标准（服务），按差额定律累进法的标准计算后下浮 20%向成交供应商成交服务费用。

### 成 交 服 务 收 费 标 准

| 服务类型 / 费率 / 中标金额（万元） | 货物招标 | 服务招标 | 工程招标 |
|---|---|---|---|
| 100 以下 | 1.5% | 1.5% | 1.0% |
| 100-500 | 1.1% | 0.8% | 0.7% |
| 500-1000 | 0.8% | 0.45% | 0.55% |
| 1000-5000 | 0.5% | 0.25% | 0.35% |
| 5000-10000 | 0.25% | 0.1% | 0.2% |
| 10000-100000 | 0.05% | 0.05% | 0.05% |
| 1000000 以上 | 0.01% | 0.01% | 0.01% |

特此承诺！

承诺方：_____（承诺方盖章）

承诺日期：

## 关于磋商保证金的声明（格式）

**（退磋商保证金使用，请单独密封，无需与响应文件装订在一起）**

**致：北京国际招标有限公司**

我单位参与贵公司组织的市局 2026 年购买移动警务服务项目，项目编号 0610-2641NF051066 。在竞争性磋商活动结束后，请将磋商保证金退至我单位以下账户：

户　　名：_____
税　　号：_____
地　　址：_____
电　　话：_____
开 户 行：_____
行　　号：_____
账　　号：_____

为此，我单位声明：

以上账户信息真实有效，如我单位相关信息在此期间内发生变更，我单位负责及时通知贵公司。如由于填写信息不实、内容不清晰、我单位信息变更而未及时告知贵公司等问题，引发的退还保证金延误等问题，后果由我单位自行承担。

供应商名称（盖章）：_____

日期：　　年　　月　　日

注：

1、　此笔款项为本项目的磋商保证金。

2、　本声明需加盖供应商公章或财务专用章，并请勿加盖在银行信息上。

3、　此声明需与响应文件一并递交。