濮 阳 市 政 府 采 购

文件编号：濮财市直竞谈-2023-23

竞争性谈判文件

濮阳市政府采购中心

2023 年 9 月 19 日

目　　录

第一部分 谈判邀请函

一、采购项目：濮阳市公安局公安网终端安全管控系统及数字证书升级项目

二、文件编号：濮财市直竞谈-2023-23

三、预算：1634765.24 元

四、采购项目需要落实的政府采购政策：

①为促进中小企业发展，根据《中华人民共和国政府采购法实施条例》“第六条”、根据财政部《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19 号）的规定，给予提供的货物全部由符合政策要求的小微企业制造的，投标报价给予 20%的扣除，用扣除后的投标报价参与评审，中小微企业划型标准见《关于印发中小企业划型标规定的通知》（工信部联企业[2011]300 号），投标人提供《中小企业声明函》（格式见招标文件附件）。

②监狱企业视同中小型企业，享受中小型企业同等政策待遇。监狱企业参加政府采购活动时，应当提供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没有提供《中小企业声明函》的供应商将被视为不接受投标总价的扣除，用原投标总价参与评审。政府强制采购节能产品强制采购、节能产品及环境标志产品优先采购。

④政府采购合同融资是河南省财政厅支持中小微企业发展，针对参与政府采购活动的供应商融资难、融资贵问题推出的一项融资政策。贵公司若成为本次政府采购项目的中标成交供应商，可持政府采购合同向金融机构申请贷款，无需抵押、担保，融资机构将根据《河南省政府采购合同融资工作实施方案》（豫财购〔2017〕10 号），按照双方自愿的原则提供便捷、优惠的贷款服务。

贷款渠道和提供贷款的金融机构，可在河南省政府采购网“河南省政府采购合同融资平台”查询联系。

五、项目基本情况：详见电子标书附件。

六、投标人及项目资质服务要求：

①符合《中华人民共和国政府采购法》规定，具有独立承担民事责任能力。

②2021 年度或 2022 年度经审计的财务审计报告或财务报告（自批准之日算起，成立不足一年，仅需提供财务报表）。

③参加政府采购活动前三年内，在经营活动中无重大违法记录。

④2022 年度 6 月份以来任意三个月缴纳税收或社会保障资金的证明（依法免税或不需要缴纳社会保障资金的供应商应提供相应的证明文件）。

⑤通过“信用中国”网站（www.creditchian.gov.cn）和中国政府采购网（www.ccgp.gov.cn）进行信用查询，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”的投标人将被拒绝参加投标活动。

供应商在投标（响应）时，按照规定提供相关承诺函（详见附件），无需再提交上述证明材料。

⑥本项目不接受联合体投标。

七、获取电子竞争性谈判文件事项：

本次采购活动通过濮阳市公共资源电子化交易平台进行信息发布、谈判文件的获取、投标文件的制作以及递交、开标、评标、结果公示实行全程电子化。

1、时间：公告发布之日起至响应文件递交截止时间前

2、地点：濮阳市公共资源交易平台(http://www.pyggzy.com/)

3、方式：登陆濮阳市公共资源交易平台(http://www.pyggzy.com/)下载招标文件；

4、售价：无

八、投标保证金：不收取。

九、响应文件提交的截止时间及地点、电子标投标注意事项：

1、时间：2023 年 10 月 8 日 9 时 30 分（北京时间）。

2、地点：濮阳市公共资源交易平台(http://www.pyggzy.com/)（综合开标室(2)）。

3、投标文件递交方式：网上递交

4、下载采购文件：凡有意参加投标者，需在公告规定时间，进入濮阳市公共资源交易平(http://www.pyggzy.com/)，凭企业数字证书（USBKEY）登录，获取电子招标文件及其它招标资料，此为获取电子招标文件的唯一途径。

5、供应商上传的电子加密投标文件，需由供应商按时网络进入与本项目相匹配网上开标室，按指令进行解密。如未在规定时间内解密电子投标文件，其投标将被拒绝。

6、投标文件递交流程：供应商登录濮阳市公共资源交易(http://www.pyggzy.com/)点击“政府采购”进行登录，选择所投项目，上传加密后的电子投标文件。如对已上传的电子投标文件进行修改，供应商可以重新上传。供应商必须在投标文件提交截止时间前完成所有投标文件的上传，逾期上传视为网上投标无效。

7、本次交易项目实行全流程电子化，投标人（供应商）不需到现场参加投标活动。实行远程解密及网上提交二次报价。各投标人（供应商）需要自备计算机且保证网络畅通，能够登录濮阳市公共资源交易平台(http://www.pyggzy.com/)（注：使用IE浏览器）。插入CA数字证书打开投标人界面，参加网上投标活动。各投标人（供应商）需通过网络密切关注项目交易全过程，所有交易环节材料均依据电子文件为准。

远程解密及提交二次报价时间：远程解密（解密时间自投标截止时间始30分钟结束）、提交二次报价（自下达二次报价命令始30分钟结束），由于投标人（供应商）错过解密、报价时间或其他自身原因导致远程解密不成功或者二次报价不成功，责任均由投标人（供应商）自行承担。给各潜在投标人（供应商）带来不便，请谅解。

十、响应文件的开启时间及地点：

1、时间：2023年10月8日9时30分（北京时间）。

2、地点：濮阳市公共资源交易平台(http://www.pyggzy.com/)（综合开标室(2)）。

十一、发布公告的媒介及公告期限：

本次公告在《河南省政府采购网》《濮阳市政府采购网》《濮阳市公共资源交易平台》(http://www.pyggzy.com/)上发布。

公告期限为三个工作日。

十二、联系方式：

1、采购人（采购文件的质疑答复人）：濮阳市公安局

地址：濮阳市胜利中路16号

联系人：李庆国

电话：13213491010

2、采购代理机构：濮阳市政府采购中心

地址：濮阳市中原路和开州路交叉口向北 50 米路东

联系人：王亚辉

联系方式：0393-6966099

3、监督单位：濮阳市财政局政府采购监督管理科

地址：濮阳市华龙区古城路中段 260 号

联系方式：0393-6666735

发布人：濮阳市政府采购中心

发布时间：2023 年 9 月 19 日

第二部分 谈判项目要求

序号	条款名称	编列内容
1	项目名称	濮阳市公安局公安网终端安全管控系统及数字证书升级项目
2	资质要求	见谈判邀请函
3	资质证件	谈判文件中须提供以下证件资质的电子档：营业执照、法人授权书、授权代表身份证及谈判邀请函要求的其他证明材料。
4	供应商要求	参加本次谈判的供应商必须由法定代表人或委托代理人（不超过 2 人）网上参加谈判，并随时接受谈判小组网上询问，并予以解答，否则将拒绝谈判。
5	付款方式	验收合格后支付合同款的 70%，一年运维服务结束支付合同款的 20%，三年运维服务结束支付合同款的 10%。
6	履约保证金	本项目不收取履约保证金。
7	供货（服务）日期	签订合同后 30 日历天完成项目建设。
8	询问和质疑	1、投标人认为采购文件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七个工作日内，以电子文档的形式向采购人提出质疑。 2、投标人认为采购程序和中标、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七个工作日内，以电子文档的形式向濮阳市政府采购中心提出质疑。
9	小、微企业、监狱企业优惠政策	见邀请函
10	电子投标文件的编制、递交	1. 投标文件全部采用电子文档（.GEF 格式），电子投标文件在网上进行上传。在投标文件递交截止时间前，投标人（供应商）登陆交易平台后，将已固化加密的电子投标文件通过网上递交的方式在投标专区自行递交，并确保递交成功（为保证文件正常递交，请投标人错峰上传， 2. 详细操作可参“濮阳市公共资源交易平台 http://www.pyggzy.com/”办事服务—操作指南—投标文件制作操作指南）。 3.未按以上要求制作电子投标文件，导致投标文件无法正常打开的，按废标处理。

11	电子标书解密	解密方式：网上解密 网上解密的，投标人凭企业机构数字证书登陆《濮阳市公共资源交易平台》(http://www.pyggzy.com/)按时解密。 2.如未在规定时间内解密电子投标文件，其投标将被拒绝。 注：为保证投标文件按照谈判文件规定时间顺利递交，请谈判供应商事先熟悉网上投标程序。

第三部分　谈判须知

1、竞争性谈判文件构成。

竞争性谈判文件用以阐明项目要求、谈判程序、评定成交标准、付款方式和合同条款。竞争性谈判文件由下述部分组成：

⑴谈判邀请函

⑵谈判项目要求

⑶谈判须知

⑷项目技术要求

⑸合同（文本）

⑹附件--谈判文件格式

⑺反商业贿赂书

2、供应商谈判文件的编写

⑴电子投标文件编制

本次采购活动通过濮阳市公共资源电子化交易平台，进行，信息发布、招标文件的获取、投标文件的制作以及递交、开标、评标、结果公示实行全程电子化。

投标人凭企业机构数字证书登录《濮阳市公共资源交易平台》(http://www.pyggzy.com/)点击登录【政府采购平台】，获取电子招标文件及其它资料。

⑵供应商应仔细阅读竞争性谈判文件的所有内容，按本文件的要求提供谈判文件，并保证所提供全部资料的真实性、有效性，以使其对本文件做出实质性响应。

3、报价应为项目最终报价，需方只承担报价，不承担报价以外的任何费用。大写金额与小写金额不一致的，以大写金额为准；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；单价金额小数点有明显错位的，应以总价为准，并修改单价。

任何有选择性品牌、选择性报价、低于成本价或者高于市场价（投标人不能合理说明或者不能提供证明材料）的，均被视为无效报价。

5、投标人发生下列情况之一，将被按照相关规定进行处理并予以公布：

（1）供应商恶意串通（标书出现雷同、加盖非本公司公章等）、提供虚假材料、不填写数据或未加盖单位公章造成废标者。

（2）成交供应商因其自身原因在接到成交通知书未能按规定时间与需方签订合同。

6、谈判文件的规定

供应商应认真阅读、并充分理解谈判文件的全部内容（包括所有的补充、修改内容、重要事项、格式、条款和技术规范、参数及要求等），供应商没有按照谈判文件要求提交全部资料，或者竞争性谈判响应文件没有对谈判文件在各方面都做出实质性响应是供应商的风险，有可能导致其谈判文件被拒绝，或被认定为无效响应或被确定为响应无效。

8、递交谈判文件的加密上传。

按规定供应商网上提交投标文件电子版。

9、谈判文件的递交

（1）电子投标文件递交方式：网上递交。

（2）投标人凭企业机构数字证书登陆《濮阳市公共资源交易平台》(http://www.pyggzy.com/)点击【政府采购平台】进行登陆，然后选择所投项目，上传签章并加密后的电子投标文件，

（3）投标人必须在投标截止时间前完成电子投标文件的上传，投标截止时间前未完成电子投标文件上传的，视为投标无效。

10、递交谈判文件的截止时间

谈判文件的递交截止时间与谈判开始时间见采购公告。

11、迟交的谈判文件

采购方将拒绝在谈判文件递交截止时间后递交的谈判文件。

12、谈判文件解密

（1）网上解密的，投标人凭企业机构数字证书登陆《濮阳市公共资源交易平台》(http://www.pyggzy.com/)按时解密。

13、谈判程序

（1）竞争性谈判可以根据项目情况采取多轮谈判，濮阳市政府采购中心在谈

判邀请函规定的时间和地点组织谈判。

（2）谈判小组对上一轮谈判中所提出的问题与供应商进行下一轮网上谈判，在谈判中谈判内容均没有实质性改变的，响应文件能够详细列明采购标的的技术、服务要求的，谈判结束后，谈判小组应当要求所有继续参加谈判的供应商在规定时间内网上提交最后报价，最后报价不能超过上一轮报价。提交最后报价的供应商不得少于 3 家。

（4）在谈判过程中，谈判小组可以根据谈判文件和谈判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，但不得变动谈判文件中的其他内容。实质性变动的内容，须经采购人代表确认。对谈判文件作出的实质性变动是谈判文件的有效组成部分，谈判小组应当及时通知所有参加谈判的供应商。

（5）供应商应当按照谈判文件的变动情况和谈判小组的要求重新提交响应内容，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

（6）谈判小组认为排在前面的中标候选供应商的最低投标报价或者某些分项报价明显不合理或低于成本，有可能影响服务质量和不能诚信履约的，在规定时间内提供书面说明材料，无法在规定时间提供说明的谈判小组可以取消该投标人的中标候选资格，按顺序由排在后面的中标候选供应商递补，以此类推。评标价及技术指标相同的，由谈判小组集体研究处理。

14、谈判小组

濮阳市政府采购中心将根据本次采购项目的特点组建谈判小组，其中专家的人数不少于成员总数的三分之二，谈判小组对谈判文件进行制定、审查、澄清、评估和比较。

15、成交原则

（1）谈判小组将遵循公开、公平、公正的原则对待每个参加谈判的供应商。

（2）严格按照竞争性谈判文件的要求，根据质量和服务均能满足采购文件实质性响应要求且最终报价最低的原则确定成交供应商。

16、供应商应自行承担所有与参加谈判有关的全部费用。

17、保密及其他注意事项

（1）在谈判期间，供应商不得向谈判小组成员询问其它供应商的谈判情况，不得进行旨在影响成交结果的活动。

（2）为保证成交结果的公正性，谈判期间直至授予供应商合同时，谈判小组成员不得与供应商私下交换意见。在谈判结束后，凡与谈判情况有接触的任何人不得将谈判情况扩散出谈判小组成员之外。

（3）不向未成交方解释未成交原因，不退还谈判文件。

18、成交通知

谈判结束后由濮阳市政府采购中心签发成交通知书，“成交通知书”将作为签订合同的依据。

第四部分 项目要求

濮阳市公安局
终端安全管控系统和公安数字证书升级项目

建设方案

2022 年 7 月

目　录

建设背景

党的十八大以来，习近平总书记就网络安全和信息化工作，提出了切实提升网络安全防护能力，筑牢国家网络安全屏障的方针号召，要求通过树立正确的网络安全观，强化关键信息基础设施安全保护，完善网络安全监测预警和应急响应机制，提高应对重大网络安全事件的能力，进而构筑坚实的网络安全屏障。

在全省公安信息网网络安全工作座谈会上也指出全省“一机两用”、违规外联等网络安全风险仍有高发势头，要求各省辖市公安局要认清当前公安信息网面临的安全形势，针对存在的突出问题，理顺思路、明确责任、坚定目标、结果导向，采取多项措施全面加强网络安全管理工作，以强烈的责任感、使命感进一步做好公安网络安全防护各项工作。要紧紧围绕网络安全防护这一主线，以党委网络安全责任制为基本原则，以网络安全大检查、突出问题专项整治为抓手，夯实网络安全防护根基，统筹推进各项工作落实。坚定信心、转变工作方法、加强工作落实一要不断坚定信心、坚持目标导向。

一 现状与问题分析

1.1 网络安全现状分析

濮阳市公安信息网建设了基于 PKI 的身份认证系统、边界接入平台、应用日志安全审计系统、“一机两用”监控与补丁分发系统等基础防护措施，但缺乏整体的保障体系。

2006 年，公安部在全国范围内进行了公安信息通信网联网设备安全管理系统（简称“一机两用”系统）的部署，该系统从系统及网络底层方面，有效的阻断了公安网终端设备遭受病毒或黑客的攻击，同时实现对设备违规外联、“一机两用”等有可能造成失泄密风险事故的风险管控，系统按照“部-省-市”三级级联的业务逻辑架构进行部署，行之有效的对接入公安信息网的终端设备相关数据进行了级联上报，确保公安信息网终端资产资源的清晰可控。该系统作为濮阳市公安局主要的终端管理系统沿用至今，承载了濮阳市局 90%以上的公安网终端运维管理工作。

1.2 问题分析

结合市局技术支撑能力实际情况，在终端安全管控系统加固及公安数字证书升级改造方面，存在以下问题：

1.终端安全管控系统新增侦听器为重要考核项，如何双机热备部署保障考核要求的问题。

2.Windows 客户端、Linux 客户端、信创客户端的兼容适配问题。

3.如何管理操作系统、数据库、网络设备等各种 IT 资源的帐号、认证、授权和审计的集中管理和控制。

4.终端安全管控系统部-省-市三级架构部署改造部-市两级架构部署的问题。

5.如何更好的使用终端安全管控系统进行系统加固及日常运维的问题。

6.如何提高新公告平台中联网设备管理及考核指标提供的问题。

9. 警务云平台未部署数据库白名单、数据库审计等安全技术措施，存在非法数据访问无法安全审计追溯的安全风险。

10.主动安全检测及响应措施缺失，难以形成有效的联动防护，信息安全实时监测和主动动态防护能力不足，难以有效发现和应对不断变化的、动态的安全风险。

1.2.1 公安数字证书升级，业务扩容能力薄弱

同步推进新一代公安数字证书的适配升级工作，以解决国产化终端用户通过 PKI/PMI 系统安全可信的接入公安网开展警务工作的需要。但该证书设备需要通过与国产化终端系统底层、驱动层、业务层、数据层的调试对接后，才能安全稳定的支持用户数字身份的认证工作。新证书同时需要向下兼容 windows 平台及 linux 平台的身份认证。在业务层面，需要兼容旧版本证书网关的认证、授权及管理等。

1.2.2 管控系统架构复杂，部署技术力量薄弱

新版本终端安全管控系统从业务架构、技术架构、网络架构等方面均与当前公

安网运行的版本不同。新版本安全管控系统需要将旧版本的部-省-市三级部署架构改造成部-市两级部署架构，联网平台需要由旧版本终端安全管控系统的单机环境部署变成集群架构部署；平台的部署支撑环境也从 windows 环境变为 Linux；联网平台的集群组件多达 20 多个。软硬件环境如果由非原厂人员部署，可能会造成系统组件不能正确安装，linux 底层服务不能有效启动，进而导致系统异常或误报风险的发生；同时，新版本的终端安全管控系统需要增加侦听器级联设备，该设备为集成度较高的一体化专用设备，由专用硬件、专用组件、专用应用及专用系统镜像组成，设备设施内部结构复杂；业务部署方面，该设备需要部署在核心交换出口处读取镜像数据；同时需要配置相关的安全策略、级联策略等，完成与部级一级总控、考核平台等专用平台的级联对接。

1.2.3 国产终端系统复杂，适配安装能力薄弱

全市公安机关国产化终端存在多批次采购配发的情况，基于国产化终端接入公安网使用的需求，需要对终端进行终端安全管控系统（一机两用）客户端软件的适配、安装、测试、调试、封装、发布等技术处理。且软件的安装部署调试等均需要通过命令行方式进行，端口的编辑及防火墙策略的开启也需要通过非图形化界面进行调试及初始化。由于国产化终端的特殊性，市级公安机关无法完成对国产化终端设备客户端软件的适配、调试及安装工作；

1.2.4 老旧终端配置杂乱，注册调优能力薄弱

目前市级公安机关尚有较多的 Linux、windows 系统的终端设备，在替换和部署终端安全管控系统客户端时，可能因计算机硬件配置、操作系统版本、设备使用年限、网络环境等内外部环境引起客户端功能性异常，如无法及时处理，可能对终端民警的正常工作造成影响。市级公安机关不具备终端软件调试、优化、封装、发布的能力；

1.2.5 新旧系统迁移合并，需业务推进平滑过渡

终端安全管控系统部署完成后，需要按照《9100 和 9200 服务器合并方案》要求，稳健迁移旧平台至新平台中，在此期间，需保障新旧平台的双活，并且对新旧平台上的设备进行“一机两用”的监控管理，避免因升级过程中出现网络中断的问题。在完成新平台自动上报的组织机构信息进行逐项梳理和修正，对冗余的保护设备信息进行清理。备份旧版“一机两用”数据并关闭扫描功能。新旧系统迁移合并，涉及专业技术及技术细节较多，市级公安机关无法实现新旧平台的平滑过渡迁移。

1.2.6 终端安全管控风险，需前置感知预警手段

终端安全管控系统“一机两用”加固版系统升级完成后，需要实时关注专用侦听器的安全策略更新、级联状态等有关考核的技术指标；需要基于专用侦听器设备的增强功能，针对接入公安信息网但未管控的终端及相关的安全风险行为，进行提前发现、感知及前置处理，进而提高安全效益，降低考核不合规的风险。市级公安机关无基于安全风险感知的前置手段。

1.2.7 终端安全运维管理，需可靠技术手段保障

终端安全管控系统加固版系统是重新开发设计的，系统通过分布式集群架构进行部署，管理器、扫描器及侦听器分别在不同的环境中运行，系统的业务架构、逻辑架构、网络架构、安全保障体系等，均不同于旧版本的系统，在维护上，需要结合故障，进行故障点位的逐点逐级排查、快速修复，通过建设健全完整的设备/系统的巡检机制，对可能出现或者已经显露的故障风险进行提前干预，避免较大系统故障或者安全故障的发生；另需满足部、省两级基于二十大安保或相关重大活动对全省公安业务的连续性考核要求。由于市级公安机关科技信息化支队人员配置不足，专业技术力量薄弱，无法基于安全运维管理的需要，提供可靠的技术、业务保障支撑；

二 需求分析

2.1 平台的需求

结合公安厅下发的“一机两用”系统和公安数字证书升级部署工作的相关通知和《“一机两用”V9200 版系统部署技术要求》的相关要求，同时结合濮阳市公安终端安全管控的及数字证书认证业务的实际情况，需要完成数字证书的适配、证书网关的接入、证书认证能力的横向扩容、终端安全管控客户端的国产化适配、终端安全管控两级架构改造、侦听器级联、数据平滑迁移、安全感知前置等业务的实施推进。结合当前旧版系统的运行状态、自身网络运行状态、硬件环境的支撑状态、技术服务能力范围等客观情况，通过依托专业技术厂商提供的软件系统的适配、测试、调试、封装、发布、部署、可靠运维的服务，完成濮阳市公安局终端安全管控系统及公安数字证书升级改造的建设部署工作。

2.2 国产化终端适配的需求

目前，濮阳市公安局陆续配发的国产化终端，在接入公安信息网的时候，基于安全可控及信息防护的需要，需要对国产化终端进行终端安全管控客户端（一机两用）软件的适配安装，同时升级的新一代公安数字证书，也需要与国产化终端进行兼容性适配。由于国产化终端操作系统的版本较多，硬件配置也千差万别，需针对各地市采购的国产化终端差异进行个性化的适配工作，并需要伴随国产化终端生命周期内的系统更新，进行相应的终端安全管控客户端升级及数字证书的升级。针对国产化终端的适配部署维护升级等工作，需要由专业的技术厂商进行专业化的适配支持工作以及持续跟踪并维护终端安全管控客户端的升级工作；

2.3 系统架构改造的需求

当前公安网运行的终端安全管控系统为部-省-市（区县）三级级联架构，加固版终端安全管控系统为部-省市（区县）两级级联架构。系统组件需要由原来的单台管

理服务器端+客户端升级改造为集群服务器端+侦听器+多种类客户端的模式；硬件环境需要由单台基础性能的服务器变更为多台高性能服务器集群及侦听器硬件的分布式集群架构；管理平台运行环境由传统的 Windows 环境升级为 CentOS 或国产操作系统环境，系统架构、技术语言及技术实施路线均需要专业的技术厂商进行专业化的部署支持；

2.4 新旧证书平台兼容的需求

新一代的公安数字证书，具备支持 SM1、SM2、SM3、SM4、SSF33 等国密算法以及 RSA1024/2048 等国际算法的能力，向下兼容 windows 平台用户的数字身份认证，但是，目前市局旧版本的证书认证网关已达到授权认证的上线，且无法对新一代的公安网数字证书进行认证、签发，需改造接入新的证书签发平台，实现证书认证能力的横向扩展、业务处置能力的纵向兼容以及新平台的统筹纳管。

2.5 可靠性改造的需求

加固板终端安全管控系统及数字证书系统升级改造期间，需要保证原有终端安全管控系统及数字证书认证的稳定运行，在加固版终端安全管控系统管理平台搭建完成后，需将旧版本系统无缝迁移至新的系统中去，在此期间，除需保证系统统连续性考核要求外，还需保障重大活动安保或突发任务状态下对系统稳定性的要求；

2.6 业务能力扩展的需求

目前配发的终端安全管控软件功能单一，且公安部制定的安全规范要求较高，配发的软件无法满足市局日益严峻的安全管理工作需要，还需要增加终端安全加固功能、安全管理等功能手段，以此发现公安信息网违规行为，从而大幅提高公安信息网安全管理能力，降低公安信息网安全管理风险。增加功能后实现我市公安信息网国产设备的统一安全管理，规范国产终端、服务器、哑终端设备接入和使用流程，对违规外联互联网、违规使用公安信息网资源等行为进行有效的监控、预计和阻断

【见下表】。

公安终端安全管控系统（一机两用）各版本功能对比表				
	基础版	加固版		
序号	基础功能	基础功能	终端安全加固功能	安全管理功能
1	违规外联监测	违规外联监测	终端禁用IPV6协议	IE设置策略
2	网关接入认证配置策略	网关接入认证配置策略	禁用终端WIFI功能	系统运行资源监控
3	网络水印管理和认证策略	网络水印管理和认证策略	禁用移动手机网络	垃圾文件清理
4	终端信息采集策略	终端信息采集策略	禁用终端DHCP功能	系统自动关机
5	终端数据收集策略	终端数据收集策略	禁用终端HTTP代理功能	流量控制策略
6	重新注册设备策略	重新注册设备策略	禁用iphlpsvc服务	文件分发策略
7	硬件控制策略	硬件控制策略	禁用终端PPPOE协议	可移动存储管理策略
8	进程监控策略	进程监控策略	终端离网锁定功能	安全刻录及审计策略
9	软件安装监控策略	软件安装监控策略	IP/MAC地址绑定功能	数据泄露行为控制策略
10	公安U盘终端注册管理策略	公安U盘终端注册管理策略	终端多网卡状态监测及禁用	安全桌面管理
11	开关机配置策略	开关机配置策略	多操作系统检查	桌面水印管理
12	警员身份认证提醒策略	警员身份认证提醒策略	边界检查策略	屏幕水印管理
13	设备使用策略	设备使用策略	用户权限管理	软件水印管理
14	公安开机提示策略	公安开机提示策略	注册表监控策略	Windows正版化检查策略
15	文件分发策略	文件分发策略	注册变检查策略	安全基线检查策略
16	消息推送策略	消息推送策略	WIFI监控策略	杀毒软件配置
17	托盘配置策略	托盘配置策略		共享监控策略
18	客户端参数配置策略	客户端参数配置策略		共享文件夹管理策略
19	客户端代理扫描策略	客户端代理扫描策略		ARP防护策略
20	客户端迁移策略	客户端迁移策略		端口检查策略
21	客户端卸载策略	客户端卸载策略		公安开机提示策略
22				托盘配置策略
23				屏幕录像策略
24				终端截屏策略
25				文件输出审计
26				文件保护及审计
27				文件内容检查
28				上网痕迹检查
29				邮件审计策略
30				终端信息采集策略

【表：一机两用功能对照表】

2.7 面对新技术发展缺乏有效防护手段

随着云计算、大数据、物联网、人工智能等新兴技术应用不断融入濮阳市公安信息化之中，传统的边界划分、边界属性鉴定越来越模糊，区分公安信息网不同的业务系统边界愈发困难，传统的边界防护体系面临着严重威胁，数据资源大量汇聚、集中存储以后，信息泄露、滥用等安全风险逐步加大。此外原有的基础安全防护措施也很难在云计算、大数据环境下实现对业务应用及数据的有效防护，业务应用及数据安全面临挑战。

三 项目概况

3.1 指导思想

以习近平新时代中国特色社会主义思想为指引，牢固树立总体国家安全观，认真贯彻党中央有关网络安全的决策，牢牢把握网络安全“四个坚持”原则，坚持网络安全为人民、网络安全靠人民，坚持网络安全教育、技术、产业融合发展，坚持促进发展和依法管理相统一，坚持安全可控和开放创新并重，统筹推进网络安全工作，构筑起坚实的网络空间安全屏障。按照“统一谋划、统一部署、统一推进、统一实施”的建设思想，遵循网络安全建设为人民的建设目标，加强推进公安有关网络安全化的建设。为维护人民安全、政治安全和国家安全贡献“公安安全”。

3.2 建设目标

基于濮阳市公安局公安信息网，构建自主可控、安全高效的终端安全管控系统及公安数字证书系统，通过升级业务架构、服务架构、网络架构及安全保障体系，实现集约化建设、融合式发展、扁平化服务的建设目标。

3.3 建设依据

安装部署适配及数据迁移、运维管理服务，因涉及到平台部署、组件部署、数据管理、定制开发等，需要基于相关的技术规范和要求进行展开，包含通用性规范及专用性规范：

3.3.1 通用性规范

（1）《关于推进公安信息化发展若干问题的意见》（公通字[2017]7 号）；

（2）《关于大力推进基础信息化建设的意见》；

（3）公安部《公安信息系统应用支撑平台总体方案设计》

（4）《采用 PKI/PMI 技术的公安应用系统安全建设技术指导书》

（5）《河南公安数据标准管理规范》（HNGA/T 0001-2016）

（6）《信息系统安全管理要求》GB/T20269-2006

（7）《信息安全技术 服务器安全技术要求》（GB/T 21028-2007）

（8）《信息安全技术操作系统安全技术要求》（GB/T 20272-2006）

（9）《数据库管理系统通用安全技术要求》（GB/T20273-2006）

（10）《中华人民共和国网络安全法》

3.3.2 专用性规范

（1）《全国“一机两用”监控系统升级工作流程》

（2）《河南省公安厅关于一机两用系统和公安数字证书升级部署的通知》

（3）《“一机两用”V9200 版系统部署技术要求》

3.4 建设原则

（1）六统一原则

按照统一运行网络、统一基础设施、统一数据资源、统一服务平台、统一安全策略、统一标准规范“六个统一”总体要求，实现“一机两用”监控平台的平滑演进。

（2）先进实用原则

平台所采用的的技术具有先进性、成熟性和前沿性。选用稳定可靠且通用的系统软件、工具软件开发平台，选用技术领先、设备先进、质量可靠、性能价格比合理的硬件。

平台所采用的技术应遵循实用性原则，满足公安行业业务需求是平台的基本目标。

平台的设计和开发充分考虑到实战的需要，以满足各警种应用需求为出发点，力求系统健壮实用。

（3）易用性原则

平台的设计贴近用户实际工作，减化用户操作流程、操作步骤和输入内容，减

轻公安的工作负担，提供详尽的用户操作手册及指导材料供用户查询使用，保证系统的易操作、易理解、易控制。

（4）传承创新原则

一方面本次建设要依托现有条件进行传承发展，客观全面分析濮阳市局的情况，做到充分利旧；另一方面本次建设要通过积极吸纳新技术、新架构、新模式结合建设实际进行大胆创新，力争把本次建设打造成“一机两用”监控平台的标杆工程。

（5）安全可控原则

平台应有完整的、统一的用户权限管理机制，防止非法访问、越级访问和非法操作，同时提供安全日志的功能。本次建设将充分考虑到公安业务的特殊性，将用户分为不同权限等级，并支持使用 PKI/PMI 数字证书登录，保证系统数据信息项的安全。

3.5 建设任务

以习近平新时代中国特色社会主义思想为指引，以牢固树立总体国家安全观为实施纲要，按照党中央有关网络安全“四个坚持”要求，基于安全可控，稳定高效的建设目标，参照公安部、省两级下发的《全国“一机两用”监控系统升级工作流程》、《河南省公安厅关于一机两用系统和公安数字证书升级部署的通知》、《“一机两用”V9200 版系统部署技术要求》等文件的指示精神，遵循分层解耦、异构兼容、充分利现、安全可控的原则，实现濮阳市公安局终端安全管控系统及公安数字证书系统的平滑演进，主要建设任务如下：

1、搭建终端安全管控系统及公安数字证书系统的硬件部署环境，以濮阳市公安局公安信息网为依托，按照《“一机两用”V9200 版系统部署技术要求》文件中对硬件设施、网络设施的要求，进行本地硬件资源、网络资源的支撑能力的评估；

2、按照《9200 升级单位基础数据报送表》要求，协助本地管理员对本地资产进行填写上报等；

3、按照《“一机两用”V9200 版（管理器、扫描器）系统安装手册》、《“一机两用”V9200 版（侦听器）系统安装手册》、《“一机两用”V9200 版（侦听器）

系统配置说明》完成部署“一机两用”9200 管理器、扫描器、侦听器并完成基本配置；

4、按照《“一机两用”V9200 版客户端安装及升级手册》，对当前濮阳市局各类型终端进行客户端的适配安装工作，出现安装故障的，需及时对安装包进行测试、修正、打包、发布，稳步推进安装工作；按照《9100 和 9200 服务器合并方案》要求，进行 9100 版本“一机两用”系统向 9200 系统的数据、资产等关键信息要素的迁移；

5、确保新平台的管理器和侦听器可正常级联到部总控中心并同步数据。

6、确保在新公告平台中，全市待处置设备总数低于公告中联网设备总数的 1%；

7、完成升级，向市局、部局报备停用老版本“一机两用”；

四 总体架构及功能设计

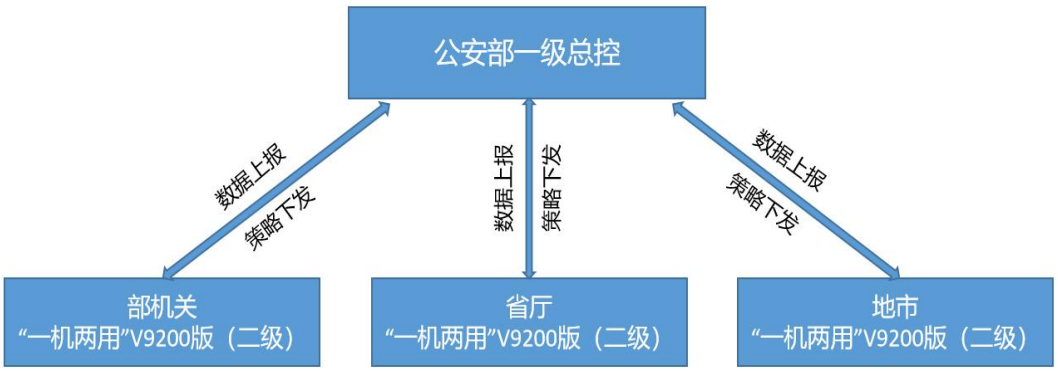
4.1 系统架构设计

公安部部署全国终端安全管控系统（一机两用）一级总控。在公安部部机关、市局厅机关和区县分别部署二级终端安全管控系统（一机两用），并级联到公安部一级总控，实现全国两级部署和管理。

服务端管理器和扫描器组件部署在一套服务器环境，实现对本级终端的安全管理。

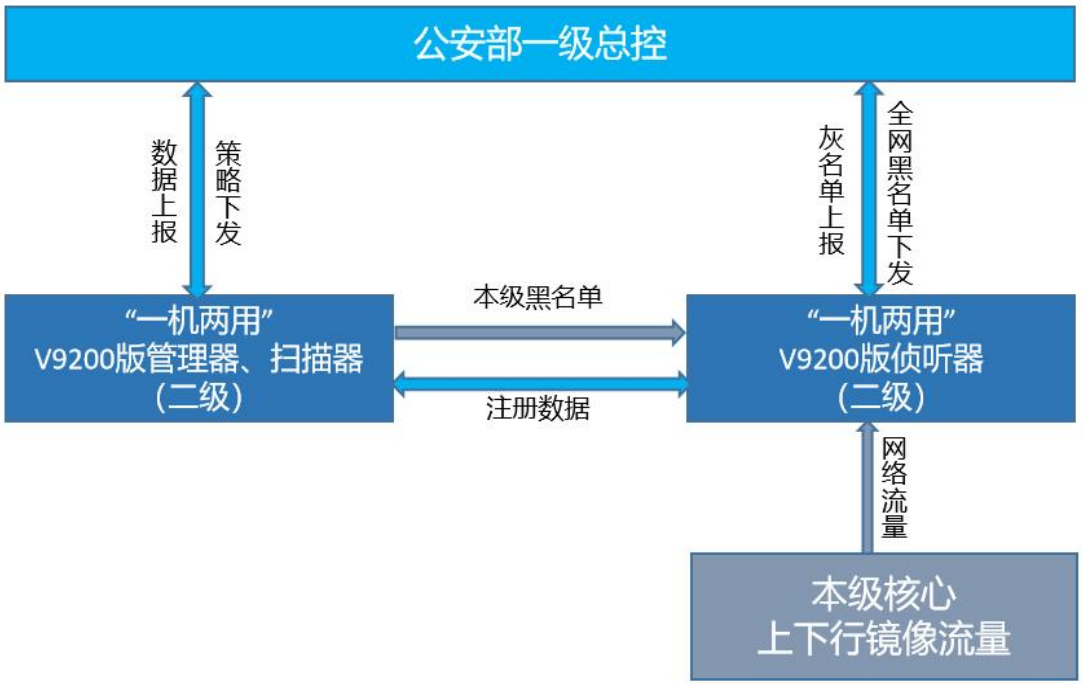
服务端侦听器组件为专用硬件设备，接收本级网络的上下行流量并与本级管理器组件和一级总控联动。

整体架构图如下：



【整体架构图】

服务端组件逻辑架构图如下：



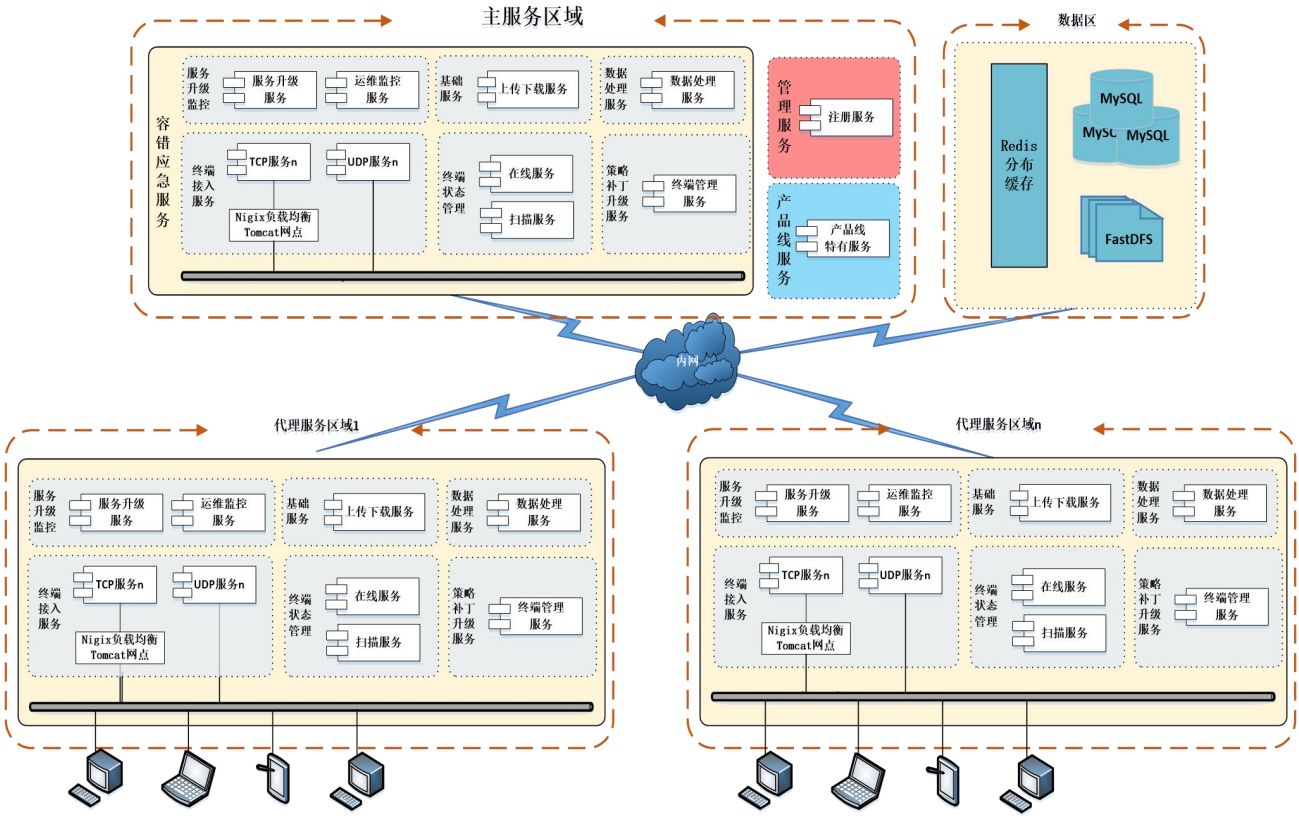
【服务端组件逻辑架构图】

4.2 部署拓扑

系统主要包括客户端、服务器端及管理平台三部分。依据 SOA 架构，采用分层结构、服务化设计，建立泛终端一体化管控平台，主要包括物理资源层、数据访问层、支撑层、服务层、业务层。其中，物理资源层包括服务器集群、分布式数据库、分布式大数据；数据访问层包括管理库、采集库、报警库及日志库等；支撑层包括应用开发框架、服务平台规范、数据访问处理等；服务层主要为后台；业务层主要

包括安全加固、安全管控、数据安全管理、资产管理、审计展示等终端管控功能模块。

系统可根据终端数量横向扩展物理设备资源，通过物理资源的扩充，实现接入能力、处理能力的提升，系统最大峰值应可支撑 300 万终端注册，200 万终端在线。业务层，终端安全管控各功能具有松耦合特征，可根据实际应用与防护需求，灵活选取及使用终端安全管理及防护功能。管理模式从多个管理端、多个客户端改变为“一个管理端+一个客户端”方式，统一管理入口，所有功能从一个管理页面配置，合并公共功能，提供统一网络通道、加密方法，节省客户端 CPU、内存、网络资源消耗。



4.3 加固版终端安全管控系统设计

加固版终端安全管控系统采用全新技术架构和部署方式，从全局角度可解决公安网长期存在的未注册设备的发现、告警和阻断问题。加固版终端安全管控系统采用服务端集群化部署方式，支持多种方式备份机制，可明显提高系统的正常运行率。

加固版终端安全管控系统支持 windows、Linux、国产化计算机等多种计算机设备的统一管理，集成终端安全服务助手、终端环境感知、移动存储介质管控等多种安全能力。

4.3.1 支持信创系统

加固版终端安全管控系统除了支持 windows 系统操作系统以外增加了适配支持信创操作系统，含 CPU（龙芯、兆芯、飞腾、神威、鲲鹏）、操作系统（中标麒麟、银河麒麟、UOS）、支持适配国产数据库和中间件，可以提供全方位的国产支持。三期目录中的平台和系统都支持，支持扩展，遇到没适配的操作系统可以支持适配。

4.3.2 支持 linux 设备

加固版终端安全管控系统支持 Linux 计算机设备（包含 linux 桌面和 Linux 服务器），新系统部署在 centos7.4 系统上，使用 Linux 服务端是目前主流趋势，Linux 服务端更加安全、更易于维护、更易于过渡到国产化系统。

4.3.3 系统业务架构升级

根据公安部的升级改造要求，加固版终端安全管控系统的业务架构，需要由旧版本的部-省-市（区县）三级级联的业务架构变更为部-省市（区县）两级级联的业务架构部署，通过业务架构的简化升级，实现高效的信息资源汇聚、提高了系统的维护效率以及稳定性等。。

4.3.4 支持多类型终端统一管理

加固版终端安全管控系统可以在同一个管理平台对多种终端进行统一管理，支持对 Windows 桌面、 Windows 服务器、Linux 桌面、Linux 服务器、信创终端、云桌面的管理。实现了在一个管理平台对多种终端统一采集资产、统一下发管理策略、统一展示数据的功能。

4.3.5 服务端可扩展性

架构上满足大数据安全对终端安全服务端的要求，响应安全管理中心的管理要求。可以支持多台服务器集群，能够支撑数十万台终端的同时管理。

4.3.6 全新的技术架构和部署方式

服务器端采用 SOA 分布式面向服务的微服务架构，具备高可用、高性能、高并发、易扩展的特性，模块间松耦合、服务间单向依赖，标准化接口和流程。终端技术架构基于 SOA 模型实现了终端功能插件化模式，方便管理和扩展其他功能模块，为一体化终端提供技术基础。

4.3.7 加固版终端安全管控系统与可信环境感知结合

加固版终端安全管控系统符合公安大数据安全设计理念，同时支持终端安全管控和可信环境感知。环境感知符合标准，支持对终端环境硬件、软件、环境风险的感知。

4.3.8 全局解决未注册设备的发现、告警和阻断问题

对联网设备的发现和管理，在全局角度建立全网多层次纵深设备发现体系。从部级开始建立覆盖全国的资产侦听机制，每个侦听器侦听全国来访资产情况，结合公安网部省市多级管理架构，采用多种先进技术实现公安网联网设备全发现，智能识别不同种类的终端，然后进行设备发现、通报、阻断。

4.3.9 增加侦听器硬件设施

加固版终端安全管控系统增加了硬件侦听器的部件，可以与公安部一级总控平台实现级联，双机热备模式，能确保与公安部保持资产设备的发现、管理等安全策略的同步更新，确保可靠通过公安部级考核要求及实现本级单位网络资产和边界的

发现，同时支持对未注册设备的发现和定向阻断，同时支持对未注册设备的引导注册。

4.4 侦听器网关设计

侦听器是公安部此次升级的重点设备，此设备承担了公安信息网的资产采集、设备发现、全国联网监控、黑灰白名单等功能，是公安信息网重点考核设备。

4.4.1 双机热备功能设计

软硬件一体化侦听器设备具备专用的双机热备接口，可通过部署 2 台设备实现系统高可用。双机热备需要配备 3 个 IP 地址，每台设备配置一个真实的管理 IP 地址，启用热备功能后两台设备以主备方式运行，对外统一提供同一个虚拟 IP 地址，用于管理的业务访问。两台设备之间热备服务相互监测设备的运行状态，当其中一台设备网络中断，业务中断，或是电源中断，设备宕机后实现自动切换。

4.4.2 资产同步及阻断功能设计

侦听器可对发现的联网设备进行设备信息识别，如设备类型、操作系统类型、设备厂商信息等。侦听器可将识别到的设备信息同步到本级终端安全管控系统管理平台资产信息列表，用于帮助管理员对未注册的联网设备进行处置判断。

侦听器可实时同步本级终端安全管控系统服务端的注册、保护设备信息，资产信息同步到侦听器设备并形成资产列表，注册和保护为本地白名单设备，侦听器通过接收流量将发现的本地设备信息与白名单资产列表进行比对，针对发现的本级未处置联网设备通过控制策略自动进行阻断。

4.4.3 违规设备发现功能设计

针对本次升级后取消了“一机两用”无效设备状态，所有终端原则上都应该为注册、保护或阻断，非此三种状态的均会被列入未处置设备，未处置设备将被部局

纳入安全管理考核。因此，为满足考核要求，部分区县级管理员可能会将大批量未处置设备设置为保护状态。保护设备一但发生“一机两用”违规事件，其考核扣分是普通“一机两用”事件的数倍。

侦听器可通过对设备信息的识别并上报至本级终端安全管控系统资产信息列表，通过高级检索分析，可对保护状态的 Windows 设备、Linux 设备、国产系统终端等进行展示，协助管理员判断不应该保护的设备被违规保护。

4.5 数字证书适配升级设计

根据《河南省公安厅关于一机两用系统和公安数字证书升级部署的通知》中对公安数字证书升级部署的要求，对濮阳市公安局民警当前使用的旧版数字证书进行升级，通过升级，实现新版本的数字证书，能够支持国密算法；对当前濮阳市局配发的国产化终端业务使用时民警身份认证的支持，同时支持 X86 架构的终端用户身份的认证。基于当前的操作系统，进行新一代公安数字证书的升级改造及配套的操作系统补丁包升级，升级后系统具有在线管理客户端，支持在线推送自动安装升级包，支持在线自动安装证书驱动，支持推送公安数字证书驱动客户端，便利后续相关的安全资产的管控对接。

4.6 公安数字证书安全认证网关扩容设计

针对市局现有数字证书安全认证网关设备老旧、支撑能力有限的客观情况，为拓展证书认证服务能力，更稳定的支持新旧版本数字证书的接入、认证及访问控制等业务工作的开展，需在市局现有证书网关的网络架构及服务能力上，通过并入新的认证网关，实现能力的拓展升级。新接入的网关设备附带 2 张公安数字证书，符合公安部关于 PKI/PMI 系统建设相关要求，网关设备性能及功能设计要求如下：

性能设计要求：配备 8 个及以上千兆电口，2U 标准机架封装，吞吐量 940Mbps 及以上，新建连接数 1089 及以上，最大并发连接数 8000 及以上；

功能设计要求：支持硬件数字证书的身份认证；支持终端特征的设备认证；支持链路服务的策略管理和下发；支持个人证书及证书 DN 项的访问控制；支持资源

的访问控制；支持 URL 的细粒度授权管理；支持黑名单动态下载功能；支持生成证书请求、申请站点证书、查看站点证书、导入站点证书、删除站点证书等站点证书管理功能；支持证书链导入、删除等证书链配置功能；支持双机热备；实现系统配置备份/恢复、日志审计等系统管理功能；支持黑名单下载服务添加、黑名单下载服务删除、支持黑名单服务查看及修改、黑名单文件上传、黑名单立即下载、黑名单文件管理、黑名单下载日志记录等黑名单管理功能；为方便运维管理快速定位故障，系统支持 Ping，Traceroute，SSH，Curl 等运维管理工具；支持公安数字证书认证，对公安用户进行权限控制与管理，随设备提供 2 张公安数字证书，证书须满足公安部关于 PKI/PMI 系统建设相关要求；

五 详细实施服务

5.1 实施步骤

终端安全管控系统加固版升级工作分为五个阶段，分别为：准备阶段、部署阶段、合并阶段、完成阶段、服务阶段。

5.1.1 准备阶段

1）、需将服务器准备情况填写到《9200 升级单位基础数据报送表》统一报送市局，再由市局报送部局。

2）、需依据《“一机两用”9200 服务端硬件环境要求》准备系统部署所需要的服务器环境。

5.1.2 部署阶段

1）、为准备的服务器安装操作系统，其中管理器、扫描器组件为 CentOS 系统或国产操作系统，安装请阅读《CentOS7.4 或国产操作系统安装手册》。

2）、服务人员将按照《“一机两用”V9200 版（管理器、扫描器）系统安装服

务步骤》，完成管理器、扫描器的部署。

3）、服务人员将按照《“一机两用”V9200 版（侦听器）系统安装服务步骤》，完成侦听器组件的部署，侦听器组件需要特定的硬件服务器设备。

4）、服务人员将按照《“一机两用”V9200 版（侦听器）系统配置说明》，完成侦听器组件的流量数据接入、策略配置、级联配置等工作。

5）、服务人员将按照《“一机两用”V9200 版客户端安装及升级服务步骤》，完成各种类型客户端的测试、封装、上载、发布、下载、安装及特殊情况下的调试工作。

5.1.3 合并阶段

(1) 在完成新一代终端安全管控系统管理平台及客户端部署安装后，经测试终端安全管控系统运行正常，服务人员将按照《9100 和 9200 服务器合并方案》，升级所有 Windows 客户端，服务端数据备份迁移，完成新老一机两用系统的合并部署工作。
(2) 为所有 Linux 设备安装 Linux 客户端。
(3) 为所有 Windows 服务器安装 Windows 服务器客户端。
(4) 为所有国产化计算机安装国产化客户端。

5.1.4 完成阶段

(1) 经市局向部局统一报备，待部局同意后，停用旧版终端安全管控系统。
(2) 完成升级工作，进入运维阶段。

5.1.5 服务阶段

在完成终端安全管控系统加固版升级部署工作后，项目整体进入到运维服务阶段。由项目服务实施单位派驻本单位一名高级软件工程师，经由终端安全管控系统加固版原厂商培训认证后，持证上岗，为濮阳市公安局提供三年期的运维服务。服

务期间，需接受濮阳市公安局科技信息化支队的管理及任务调度，同时提供系统整体运行风险的稳控工作，包括日常巡检、考核支撑、应急响应、特殊时期保通及运维日志记录管理上报等工作。

5.2 实施服务

5.2.1 数字证书适配服务

基于当前濮阳市局配发的国产化终端型号，支持对麒麟 V10 操作系统进行有关数字证书的补丁包升级，以满足新一代数字证书外设对商密算法的支持，同时支持国产化终端及 X86 客户端的数字身份认证，整体升级适配服务包括：支持在线管理客户端；支持在线自动安装升级包后；支持在线自动安装证书驱动；支持推送公安数字证书驱动客户端。

5.2.2 证书认证网关的接入

基于当前数字证书认证网关的网络部署架构、业务处置流程规范，进行新一代数字证书认证网关的拓展接入；接入的数字证书认证网关，能够兼容原有证书认证业务及对旧版本证书的授权认证，能够实现统一统筹的纳管。

5.2.3 客户端（国产化）适配

受国产化终端物料供应、产能不足以及国产化终端品牌众多的影响，各地公安采购配发的国产化终端，存在着同批次不同型号不同配置或者多批次不同型号不同配置的情况。在终端安全管控软件安装及新一代数字证书安装时，因硬件环境的不一致、不兼容，极易造成软件安装、证书驱动加载、数字签名等组件服务的安装更新失败，也可能造成软件功能受阻或安全保障功能的失效；因此，为加快终端安全管控系统整体部署的进度以及数字证书的适配进度，需要在客户端批量部署前，对用户当前配发的各版本各类型的终端进行抽样适配，在降低安装风险系数后，重新封装、发布安装包，进行批量安装。

5.2.3.1 终端抽样

针对濮阳市局当前国产化终端的适配情况，统计采购批次、型号、配置等信息，以批次为抽样大类，在每大类里，按照机型型号、机型配置为依据进行样机的抽取，总体样本比例按照濮阳市局国产化终端总数的 1%抽取；

5.2.3.2 客户端选型

根据抽样汇总的终端配置信息，参照前期终端安全管控厂家适配龙芯、兆芯、飞腾、神威、鲲鹏等平台或中标麒麟、银河麒麟、UOS、windows、linux 等操作系统发布的终端安全管控客户端，选择符合本地终端配置的客户端软件或相近配置的客户端，进行适配安装。

5.2.3.3 样本机型测试

样本机型安装终端安全管控系统加固版客户端软件并与测试系统级联后，对样本机进行违规外联、U 盘管理，病毒防护、文件管理、移动网络、多网卡等风险事故测试；对软件安装、注册配置、托盘服务、自启动等强管理项进行验证；对测试管理平台上报信息进行复合，详细记录测试结果。

5.2.3.4 客户端修复

基于样本机型测试结果，对出现不兼容或功能缺陷的终端，进行客户端二次风险事故测试同时选择同类型同配置机型进行对照测试，并详细记录测试结果。若客户端适配或功能缺失的故障依旧存在，则需通过专业厂家的技术研发力量，对软件进行功能修复；若客户端适配或功能缺失的故障不存在，则对一次报故障的机型进行三次风险事故测试，确认无故障后，则提交该机型适配的客户端类型。

5.2.3.5 客户端封装及测试

对修复的客户端进行封装，校验软件的 MD5 及数字签名，对封装后的软件进行

功能测试，包含安装、风险事故测试、强管理功能测试等，确认无误后，提交至以及市级终端安全管控系统管控平台，进行安装包资源的上载；

5.2.3.6 测试数据清理

对参与测试的样机，进行测试数据清理，将样机恢复到测试前的状态，便于正式环境下终端安全管控系统软件的安装部署服务；

清理测试管理平台的风险管理数据，便于正式环境下终端安全管控系统终端的接入监控、信息上报；

5.2.4 客户端（国产化及非国产化）安装

通过客户端适配服务确定适用于濮阳市局的客户端型号、版本，提供针对各种类型终端的安装服务，包括国产化终端及非国产化（Windows 终端及 Linux）终端；终端载体类型包括民警个人工作电脑及服务器等设备设施的安装服务；

5.2.4.1 在线安装

通过电话、邮件、短信或可用的即时通讯手段，为民警提供在线安装指导服务，包括客户端的安装、注意事项、系统注册，可根据市局整体的情况，就共性问题，统一发布安装指导类公告。

5.2.4.2 线下安装

针对已经采购但暂未下发的国产化终端，提供统一的线下安装服务，由工程技术人员到设备仓库进行逐台安装或在固定的场所进行批量安装；针对已经下发的国产化终端，且不方便在线安装的，须由所有人单独或单位统一将主机送至指定场所，由专业的技术人员进行安装；

5.2.4.3 驻地安装

由于设备安装位置的特殊性及其它客观原因，无法进行线上及线下安装的，需由专业的工程技术人员，进行驻地安装。

5.2.5 加固版终端安全管控系统的部署及质保

结合濮阳市公安局当前的网络现状、资源现状，针对加固版终端安全管控系统的实施部署，需利旧市局现有硬件支撑资源，实现管控平台管理器、扫描器的集群部署。

5.2.5.1 支撑资源准备

5.2.5.1.1 节点环境要求

终端安全管控系统加固版（管理器、扫描器），需要多台服务器实现集群化部署。服务器数量应依据本级区域终端数量配置，且每台服务器均需要配置一个公安网 IP。服务器数量与管理的终端数量关系表如下：

终端数	服务器数量	IP 地址
1000 以下	1	1 个
1 千--1 万	3	3 个
1 万--2 万	5	5 个
2 万--3 万	7	7 个
3 万--4 万	9	9 个
4 万--5 万	11	11 个

根据濮阳市公安局当前接入公安网终端数量的统计，本次升级部署需要提供三台服务器，物理机、虚拟化、云资源均可提供集群化部署支撑，节点环境要求满足 8 核 CPU+64G 内存+2T 硬盘的配置。

5.2.5.1.2 网络环境要求

需要提供的网络环境如下：

（1） 基于 3 节点集群的配置方案，全网可达的 IP 地址及网络接口 3 个；

（2） 基于侦听器热备需要，本级核心流量镜像接口需按 2 个进行配置。

（3） 基于管理平台的服务/业务需要，需开放 TCP 及 UDP 端口：

TCP:80、88、443、32122、51616、22250、51613；

UDP:8300、22116、13001

5.2.5.2 部署服务

终端安全管控系统加固版（管理器、扫描器）所部署的集群服务器，是由多个服务分散在一个或多个服务器环境中。集群的服务配置规划如下表：

节点	部署业务/服务信息
服务器 1	MySql 主数据库/Tomcat 中间件/主数据缓存节点
服务器 2	平台管理/从数据缓存节点/MySql 热备数据库/客户端接入服务/业务运算
服务器 3	客户端接入服务/业务运算/文件管理/数据上载、安全配置及策略同步更新服务

5.2.5.2.1 操作系统安装

参照平台节点的支撑系统要求，基于物理机资源，提供 Centos7.4 及以上系统的安装部署服务，提供必要的系统支撑组件安装部署服务，提供访问控制、端口设置、防火请设置、用户权限设置等相关安全管控设置服务；提供必要的虚拟机联机测试服务；针对市局的虚拟化资源或云服务资源，要求终端安全管控系统厂商配合云服务或虚拟化资源服务商提供平台支撑系统的技术规格参数，便于支撑系统的及时部署及联调联试工作的展开，要求对上述涉及系统变更的操作，进行可靠性测试，确保系统可靠访问；

5.2.5.2.2 远程文件上载

提供终端安全管控系统集群的远端文件上载服务，将主备数据库软件、中间件、负载均衡、双击热备软件、终端安全管控平台、客户端接入、业务运算、数据上载、策略更新、上报级联、文件管理等所需的文件资源上载至指定路径，要求通过用户名、密码及端口的验证的方式建立可信的安全会话，要求上述操作后进行系统可靠访问测试。

5.2.5.2.3 安全隧道连接

提供终端安全管控系统集群的安全隧道会话服务。统一设置主机进程编码 UTF-8 格式，要求通过用户名、密码及端口验证的方式安全链接远程终端，配置必要的 TCP/IP 转移规则及安装配置 xmanager 服务，根据业务部署需要，关停 SELINUX 服务，要求对上述操作进行可靠性测试。

5.2.5.2.4 解压部署安装

需技术厂商针对上载的安装文件，提供解压部署服务。根据安装文件的用途及类型，展开安装部署。提供辅助工具或组件的安装调试，包括 yum、wget、lsof、tcpdump、vim、bash 等。根据安装需要，提供组件端口修改或防火墙端口修改、添加 tcp 及 udp 监听端口等服务。根据组件或软件安装需要，编辑批量安装脚本，开放相应的端口、设置脚本自动安装权限、启动安装服务等。提供软件或组件运性必要的端口修改、添加等服务。

5.2.5.2.5 初始化

提供终端安全管控系统的初始化服务。系统各个组件安装完成后，进行图形管控系统的初始化安装；通过超级管理员或安全审计员账户，实现不同权限控制下的系统管理或安全审计管理。

5.2.5.2.6 系统初始配置

系统初始配置用于完成系统服务器端的初始配置，主要包括组织机构及管理范围、客户端参数配置、客户端安装包发布、扫描范围配置和配置外网地址。

（1） 组织机构及管理范围配置：配置组织机构及组织机构的 IP 管理范围。

（2） 客户端注册参数配置：为不同类型的终端配置不同注册界面，显示隐藏功能项，提供更多注册项用于终端注册使用。

（3） 客户端安装包发布：提供经正式安装测试完全适配濮阳市局国产化终端机型的终端安全加固客户端安装包（zip 压缩包），提供当前市局其它类型终端的客户端安装包，提供客户端升级后的更新包的上载及发布。

（4） 配置级联地址：提供与部局一级总控级联的地址、端口等参数信息的配置，能够管理本级级联服务的配置信息等。

5.2.5.3 质保

终端安全管控系统加固版平台部署完成并验收后，系统进入三年质保期，由系统承建单位提供三年原厂质保服务。质保期间，需保证系统平台的组件、数据库、集群软件、分布式软件、主被管理软件、平台应用软件、平台管理软件等涉及到的软件的质保服务，提供软件功能确实修复、补丁升级、必要性的重装或同步的安全更新等服务；需保证专用的侦听器一体化设备软件功能正常，包括各功能组件、安全策略更新、级联控制、黑灰发现、数据同步更新等；提供必要时对侦听器设备的初始化服务；提供质保期间，因软硬件故障无法修复时，同规格备品备件的免费更换服务；

5.2.6 加固版终端安全管控系统的平台监管

基于新一代微服务技术架构及专利技术体系框架，面向全警实战化应用需求，依托濮阳市公安局公安信息网资源，针对终端安全管控系统加固版系统升级后系统可靠监管运行的需求，通过构建终端安全管控系统一体化平台，提供加固版终端安

全管控系统平台的监管服务。

该平台实现了一个，提供大容量、高密级的数据处理和实时监控能力；支持采用分布式级联部署模式， 构建了统一安全管理平台，一体化解决各种终端类型在多样的系统环境中所面临的复杂安全威胁，“一套服务器，一个客户端”，涵盖主机安全、行为安全、边界安全、网络安全和数据安全、系统运维等领域，各子系统采用模块化设计，无缝集成，统一界面、集中管理。通过集群方式，在平台内部的各业务单元之间实现负载均衡，提供百万级终端的集中管控能力。在集群模式下，可实现系统数据集中于总部存储。既方便数据备份，也有效避免了级联模式下下级通过篡改本地数据库达到规避监管的目的。在系统管理上，支持由总部管理员统一管理；也支持创建子管理员账号，由子管理员分区管理；也能支持原来的级联管理模式。单个终端多产品的插件化接入，各产品使用统一的认证入口、统一的应用入口、统一的界面风格，并提供标准化的策略接口、数据总线通道、网络通信通讯协议格式。支持子产品以升级方式下发到终端，方便用户逐步扩展应用。在同一个平台提供对多种终端的管理能力，支持对 Windows 桌面, Windows 服务器，Linux 桌面，Linux 服务器，云桌面及国产终端的管控。综合统计分析多个产品的数据，深度挖掘数据价值，并提供丰富的大屏展示功能。

5.2.7 新旧终端安全管控系统的数据迁移

在加固版终端安全管控系统部署完成后，需将旧版本服务器数据资源、安全策略、资产列表等信息资源平滑稳定的迁移至加固版平台中，要求稳定迁移，保证迁移期间不影响公安业务运行，要求平滑迁移，迁移期间能保证终端安全管控平台的可靠运行，数据无缝接入；具体迁移服务如下：

(1) 旧版服务器信任保护数据向加固版服务器迁移：旧版服务器上设置信任/保护的设备信息自动同步到加固版服务器资产信息中，内容包括 IP 地址，MAC 地址，设备名称，持有人，所在地，组织机构。

(2) 通过文件分发策略分发【9100idm 防火墙卸载程序】进行旧版客户端的卸载，避免之前存在的卸载旧版客户端时网卡异常的问题。

(3) 通过旧版的软件分发模式分发加固版安装包，实现自动更新升级。针对未能分发成功的，可自行注册加固版客户端（注册客户端的同时，会自动卸载旧版客户端）并自动上传注册信息，无需人为干预。

(4) 备份旧版策略，根据旧版策略要求，在加固版服务器上建立对应的策略，并逐步分发。

(5) 注意事项

- 迁移期间，关闭旧版和加固版服务器的未注册阻断功能
- 迁移期间，旧版及加固版服务器需要共存一段时间，直到客户端全部迁移到加固版服务器，旧版的服务器建议保留三个月。

5.2.8 警用地图专题应用

警用地图专题应用能够使计算机终端、警务通移动终端、警车移动终端等信息，在地图上清晰、直观地展现出来，实现数据可视化、地理分析、安全态势分析，达到与已有业务应用的有机集成，实现多维性的需求。

警用地图专题应用系统依赖于现有的警用地图基础平台、业务系统及相关数据，并在此基础上综合利用，构建更深层次应用,主要分为基础应用和专项应用。

具体应用需求如下：

(1) 警务要素上图：综合利用地理信息技术所特有的空间分析功能和强有力的可视化表达能力,为警务信息提供快速的空间定位参考。警务要素主要包括：计算机终端；公安机关辖区；行政辖区；公安机关驻地；警力资源，如：警车及执法记录仪；归属公安管理的企事业单位及业务数据，如：网吧、旅馆等；公安建设的信息化前端采集设备及数据：视频、卡口等；公安汇聚的社会资源；

(2) 车辆轨迹展示：通过分析车辆卡口数据，根据时间范围及车辆信息，可在地图上显示出车辆行驶轨迹、车辆的基本信息等，对比表格卡口数据，更直观的显示出车辆的行驶轨迹。

(3) 警务信息检索：警务信息量大，且类型多，提供警务信息检索，支持按类型、名称、地理坐标进行查询，查询的的结果如：旅馆、网吧、视频、卡口,在地图上显示出检索结果。

点击地图上的结果支持查看该信息的详情信息。

(4) 地址信息采集：地址信息的新增、修改、删除，要显示出新增时间及新增人，任何地址信息都要经过审核后才能上图，保证图上展示的信息都是经过确认的。地理坐标信息采集分两种：支持直接在 Web 端地图上选择点或范围；新增或修改警务信息时支持直接在 Web 端地图上选择该信息的坐标信息或范围。通过移动终端定位功能采集地理坐标；通过获取移动终端的地理坐标，直接将采集的地理坐标更新到地址信息中。

(5) 基础服务：通过基础服务，将采集的警务信息更加灵活，支持警务信息的坐标信息进行转换：公安网地图坐标与互联网地图坐标互转；支持公安网地理坐标互转为:百度地图坐标、高德地图坐标。通过互转服务，可以将有些原有数据，如：百度地图或高德地图的地理坐标信息进行转换，提高系统的兼容性。按照警务要素的坐标和警务要素类型查询所属区域、所属辖区；通过辖区和警务要素类型查询辖区内所有警务要素；

(6) 地图工具：测量：用于在地图上测量长度距离。框选：用于在地图上选择面积范围。标注：可以在地图上标注绘制点、绘制线。路线规划：用于在地图上手工绘制路线。鹰眼：用于在地图缩略图中勾选中心位置。

(7) 专项应用：包括:警力分布规划、专项活动路线规划、封控圈预案规划和周边警用信息资源查询。警力分布规划：为了提高反应速度，警力分布规划可用于对：各类警车、各类警种的实时位置数据会传送到警用地图专题应用系统，并在大屏幕的地图上显示出来。遇到重大警情时，可以根据地图上警力的分布直接对各类警力进行调度 ，这种“可视”的调度过程能在最短的时间内，对犯罪嫌疑人实施围捕。专项活动路线规划：用于在执行某专项活动

时，直观的绘制行动路线。封控圈预案规划：通过封控圈预案规划工作，有序高效地落实封控圈应急处理工作，提前对封控圈进行预案规划。周边警用信息资源查询：用于在地图上查询事发点周边警用信息资源，包括视频、卡口等。

5.3 项目培训及安全运维

为保证系统平稳运行，降低考核风险、运维风险、保障公安实战业务开展、助力重大活动安保的保通工作以及系统的安全管理、及时升级的业务需要，需提供培训和运维服务。从根本上解决市局专项技术支撑能力不够，国产化终端生命周期内的适配升级服务需求等，需要 7*24 小时的安全运维服务。一方面，需要保证系统的平稳运行、另一方面需要保证系统级联公安部的正常，第三，及时发现考核风险要素，实时给予干预；第四，满足国产化终端不断升级的客户端适配的要求；第五，为公安实战业务提供可靠有力的保通作用。

5.3.1 培训

承建方按照建设单位要求，免费为最终用户进行人员培训。采用施工现场培训和主要软硬件设备生产厂商的原厂总部培训相结合的方式进行。讲课以幻灯片为主，讲授理论性的知识。日常维护、常见故障排除采用上机操作，提供所有产品的全套中文技术资料、使用手册和软件光盘，以及系统集成和实施中形成的完整文档资料。按照建设单位的时间、地点要求，针对系统管理人员、系统维护人员、系统操作人员等建设单位认为应该接受培训的人员围绕项目建设相关内容提供不同角度、有针对性的培训。

承建方需免费提供不少于 3 人的项目厂商总部或项目厂商认证的专业培训机构的系统管理员培训，培训内容包括前端设备、网络设备、软件平台等，使系统管理员能独立进行系统管理、一般故障处理、简单测试维护等工作，确保系统正常安全运行，培训场地等费用全部由承建方承担。

5.3.2 日常巡检

提供加固版终端安全管控系统、安全助手系统、侦听器等系统的安全部署及运维工作，提供每月一次的现场巡检服务，重点检查系统运行情况，切实提升一机两用监控系统正常运行率。

巡检的内容包括：

1）新补丁公布时，为全局的补丁库导入新的经过测试和病毒检测的补丁。

2）根据市局公安网的实际使用情况，对其系统安全策略进行合理的修改。

3）如果系统有升级的情况，对全局的该套系统进行相应的升级维护，并说明升级有关的具体事宜。

4）检查系统服务器的安全状况。

主要检查系统服务器相关资源的占用情况，系统自身补丁更新情况，以及对系统进行病毒检查。

5）对系统服务器报警信息的检查。

重点检查报警信息的处理情况，结合报警内容，配合管理员处理内网中主要存在的一些问题

6）培训安全管理员的产品使用技巧。

巡检过程中对系统的相关操作使用技巧、常见问题的处理等方面对管理员进行指导和培训。

7）对系统产生的数据进行备份并整理。

每次巡检时，对服务器端的数据库及相关审计日志进行备份，并对原有无用数据进行清理，以保证服务器运行的稳定性和安全性。提供数据备份服务。

8）收集使用单位对产品的良好建议，并研发分析产品进行改进。

9）每次巡检后向提供巡检报告。

5.3.3 考核现场支持

针对公安部质量运行管理考核的要求，提供现场技术支持服务

安排服务工程师，及时排除故障，每月进行一次巡检，使用专用工具对全局服务器列表进行清理，确保每月服务器漏洞扫描工作的准确性；对一机两用正常运行率、一机两用注册率、防病毒软件覆盖率等公安部考核进行技术支持。

5.3.4 应急响应

故障按影响程度分为四级，一级故障定义为：由于产品原因造成网络局部或全部瘫痪；二级故障定义为：服务器端程序无法正常运行；三级故障定义为：产品部分功能无法实现；四级故障定义为部分客户端出现异常等。

在监控到故障告警后，五分钟内给出口头应急措施，一小时内给出完整解决方案。一级故障或二级故障，在无法提供解决办法的情况下，尽可能在应急措施后先恢复网络正常。三级故障和四级故障一般以本地驻场支持的方式解决，由于产品本身原因无法解决的，提供备品备件支持服务外，另需技术厂商在 24 小时内赶赴现场负责处理。

5.3.5 特别时期的现场保通

在重要活动、或重要会议、春节前、国庆节前、五一劳动节前等特别时期，根据用户单位要求，可以提供专门的终端安全保障服务，并协助安全管理员做好终端安全的技术保障工作，确保相关活动、会议的顺利进行。

5.3.6 其它任务调度

根据有关安全工作推进的任务要求及安排。需对终端安全管控系统加固版系统二级平台的客户端注册、运行、监管、通报等数据进行整理导出的；需通过开发页面或结合 GIS 进行全市安全形势上图的；或根据领导宏观决策要求进行三方系统对接，在进行安全风险评估后，提供任务调度服务。

六 项目设备及服务清单

序号	设备名称		详细描述	数量	单位
1	加固版终端安全管控系统一体化侦听器设备	硬件性能规格	2U 一体化硬件设备；1 个 1000BASE-T 管理口，1 个 Console 口，1 个双机热备接口，2 个 USB 口，4 个 1000BASE-T 电口，2 个万兆光口，可支持扩展到 4 个万兆光口；	1	套
		侦听器功能要求	1、具备 2 路业务接入，可支持到 4 路业务接入； 2、具备与本单位“一机两用”监控系统对接能力，自动同步本地的注册资产信息，保护资产信息、阻断资产信息。 3、具备与公安部“一机两用”一级总控制对接能力，实现本地发现的灰名单资产上报和接收一级总控下发的全国黑名单资产。 4、具备对黑名单资产的阻断能力。 5、设备支持高可用，双机热备能力。可满足公安信息网安全运维考核要求。（提供完整考核要求文档） 6、数据高可用，具备黑名单资产数据定时同步能力。 7、具备资产指纹分析能力，对发现的联网设备进行详细信息识别； 8、具备对识别到的设备信息可同步到“一机两用”资产列表；（提供接口证明文件） 9、具备对未处置设备的发现和自动阻断功能。 10、提供“一机两用”系统与侦听器联调安装运维能力		
2	加固版终端安全管控系统	联网管理平台	1.联网设备管理平台升级为终端一体化系统，支持统一管理中心，可通过一个平台时实现对国产化设备及 Windows、Linux 设备的统一管理。 2、支持 C/S 和 B/S 模式混合管理方式。在安装客户端程序需要填写当前计算机使用人的个人相关信息，如使用人、机构、设备类型、设备用途等。 3、系统支持与公安部同平台部-市二级级联管理，下级支持与上级的数据上报及策略级联，上级支持实时连接下级并可实现对主机的实时控制。（提供级联接口文档）	1	套

			4、支持安全监控审计功能：上网访问行为审计、打印审计。 5、监控终端的非法连接外部网络，目前是通过设置外部网络 IP 或域名，若能连同则触发审计，支持设置外联服务器连同，并在发生外联时候直接对终端进行断网或关机处理；		
		扫描器	1、支持文件分发功能，向指定客户端分发文件，文件分发时可报告软件安装的状态。 2、支持移动存储策略管理，能够对终端移动存储设备的接口进行管理控制，支持对移动存储介质的禁用和读、写权限控制，对 U 盘使用进行管理和审计。 3、系统能够自动搜集客户端安装的所有软件信息，将相关数据入库供管理员在 Web 控制台查询。 4、支持在 Web 控制台对计算机终端的网络流入、流出和总流量进行监控和管理。并能够对产生总流量过大、分时段瞬时流量过大的终端进行统计。	1	套
		运行数据聚合	1、采集终端资产的软硬件信息：硬件 CPU、内存、磁盘； 2、支持注册率、管理中心正常率、杀毒软件覆盖率等全网考核数据的统计，支持待处理设备展示。 3、支持统一汇总展示计算机操作系统类型、终端数量、软硬件资产等。 4、支持对计算机终端的 CPU、内存、硬盘的资源占用率和剩余空间进行监控，设定危险等级报警阀门，报警信息可在管理平台统一查看。	1	套
		监管平台	基于新一代微服务技术架构及专利技术体系框架，面向全警实战化应用需求，依托濮阳市公安局公安信息网资源，针对加固版终端安全管控系统升级后系统可靠监管运行的需求，通过构建加固版终端安全管控系统一体化平台，提供平台的监管服务。该平台提供大容量、高密级的数据处理和实时监控能力；支持采用分布式级联部署模式，构建了统一安全管理平台，一体化解决各种终端类型在多样的系统环境中所面临的复杂安全威胁，“一套服务器，一个客户端”，涵盖主机安全、行为安全、边界安全、网络安全和数据安全、系统运维等领域，各子系统采用模块化设计，无缝集成，统一界面、集中管理。通过集群方式，在平台内部的各业务单元之间实现负载均衡，提供百万级终端的集中管控能力。在同一个平台提供对多种终端的管理能力，支持对 Windows 桌面, Windows 服务器，Linux 桌面，Linux 服务器，云桌面及国产终端的管控。综合统计分析多个产品的数据，深度挖掘数据价值，并提供丰富的大屏展示功能。	1	套

		加固版客户端	1、支持 Windows 客户端 Linux(CentOS 和 Redhat)客户端注册，客户端支持国产系统（UOS、中标麒麟、银河麒麟）注册。 2、支持违规外联监控功能：网络内部终端非法外联行为监控、非法外联行为取证。 3、支持 IP 与 MAC 绑定，禁止终端用户修改 IP 地址、网关等参数，并自动恢复、断网和提示等处理。支持设置可修改的 IP 范围，支持服务器同步绑定 IP/MAC，防止终端重做系统后修改 IP。 4、按照安全要求对外界硬件设备进行管控：放行、禁用、例外等操作； 5、含 1000 个 license 授权许可； 加固版功能要求： （1）基础功能：违规外联监测、网关接入认证配置策略、网络水印管理和认证策略、终端信息采集策略、终端数据收集策略、重新注册设备策略、硬件控制策略、进程监控策略、软件安装监控策略、公安 U 盘终端注册管理策略、开关机配置策略、警员身份认证提醒策略、设备使用策略、公安开机提示策略、文件分发策略、消息推送策略、托盘配置策略、客户端参数配置策略、客户端代理扫描策略、客户端迁移策略、客户端卸载策略； （2）终端安全加固功能：终端禁用 IPV6 协议、禁用终端 WIFI 功能、禁用移动手机网络、禁用终端 DHCP 功能、禁用终端 HTTP 代理功能、禁用 iphlpsvc 服务、禁用终端 PPPOE 协议、终端离网锁定功能、IP/MAC 地址绑定功能、终端多网卡状态监测及禁用、多操作系统检查、边界检查策略、用户权限管理、注册表监控策略、注册变检查策略、WIFI 监控策略； （3）安全管理功能：IE 设置策略、系统运行资源监控、垃圾文件清理、系统自动关机、流量控制策略、文件分发策略、可移动存储管理策略、安全刻录及审计策略、数据泄露行为控制策略、安全桌面管理、桌面水印管理、屏幕水印管理、软件水印管理、Windows 正版化检查策略、安全基线检查策略、杀毒软件配置、共享监控策略、共享文件夹管理策略、ARP 防护策略、端口检查策略、公安开机提示策略、托盘配置策略、文件输出审计、文件保护及审计、文件内容检查、上网痕迹检查、邮件审计策略、终端信息采集策略；	1	套
		抽样适配服务	为加快加固版终端安全管控系统的整体部署进度，提高大批量安装的工作效率，降低客户端安装给民警工作带来的迟滞风险。需要在客户端正式部署前，对用户当前配发的各版本各类型的	1	套

			终端，按照配发量的1%进行抽样，按照配发批次、配置型号、配发警种单位等多个维度进行样品分配，提供加固版终端安全管控系统客户端（国产化）适配服务，服务内容包括终端抽样、客户端选型、样本机型测试、客户端修复、客户端封装及测试、测试数据清理等，在降低安装风险系数后，重新封装、发布安装包，进行批量安装。		
		安装部署服务	提供项目部署阶段各类型终端、管控平台、监管平台、证书网关及各功能组件的安装部署服务；在项目生命周期内，提供伴随终端升级的终端安全加固客户端及数字证书的适配、升级、改造及安装部署服务 **（一）客户端部署服务：**通过抽样适配服务确定濮阳市局的客户端型号、版本，提供针对国产化终端、Windows终端及Linux终端等各种类型终端，针对民警个人电脑、服务器等各类型应用场景的设备设施的加固版终端管控系统客户端的安装服务，包括但不限于：在线安装、线下安装、驻地安装 1、在线安装：通过电话、邮件、短信或可用的即时通讯手段，为民警提供在线安装指导服务，包括客户端的安装、注意事项、系统注册，可根据市局整体的情况，就共性问题，统一发布安装指导类公告。 2、线下安装：针对已经采购但暂未下发的国产化终端，提供统一的线下安装服务，由工程技术人员到设备仓库进行逐台安装或在固定的场所进行批量安装；针对已经下发的国产化终端，且不方便在线安装的，设备所有人或由单位统一将主机送至指定场所，由专业的技术人员进行安装； 3、驻地安装：由于设备安装位置的特殊性或其它客观原因，无法进行线上及线下安装的，需由专业的工程技术人员，进行驻地安装或到设备部署地址安装。 **（二）平台部署服务：**加固版终端安全管控系统联网管理中心为集群化部署应用平台，实现管理器、扫描器等业务功能，其中包含的服务组件、中间件等技术节点。技术结构较为复杂，包括：主备数据库、中间件、主从数据缓存节点、平台管理、客户端接入负载均衡服务、业务运算负载均衡、文件管理、数据上载服务、安全配置管理、策略同步更新服务等。平台部署主要包括以下方面工作： 1、操作系统安装服务：参照平台节点的支撑系统要求，基于物理机资源，提供Centos7.4及	1	项

			以上系统的安装部署服务，提供必要的系统支撑组件安装部署服务，提供访问控制、端口设置、防火请设置、用户权限设置等相关安全管控设置服务；提供必要的虚拟机联机测试服务；针对市局的虚拟化资源或云服务资源，要求终端安全管控系统厂商配合云服务或虚拟化资源服务商提供平台支撑系统的技术规格参数，便于支撑系统的及时部署及联调联试工作的展开，要求对上述涉及系统变更的操作，进行可靠性测试，确保系统可靠访问； 2、远程文件上载服务：提供终端安全管控系统集群的远端文件上载服务，将主备数据库软件、中间件、负载均衡、双击热备软件、终端安全管控平台、客户端接入、业务运算、数据上载、策略更新、上报级联、文件管理等所需的文件资源上载至指定路径，要求通过用户名、密码及端口的验证的方式建立可信的安全会话，要求上述操作后进行系统可靠访问测试。 3、安全隧道连接服务：提供终端安全管控系统集群的安全隧道会话服务。统一设置主机进程编码 UTF-8 格式，要求通过用户名、密码及端口验证的方式安全链接远程终端，配置必要的 TCP/IP 转移规则及安装配置 xmanager 服务，根据业务部署需要，关停 SELINUX 服务，要求对上述操作进行可靠性测试。 4、解压部署安装服务：需技术厂商针对上载的安装文件，提供解压部署服务。根据安装文件的用途及类型，展开安装部署。提供辅助工具或组件的安装调试，包括 yum、wget、lsof、tcpdump、vim、bash 等。根据安装需要，提供组件端口修改或防火墙端口修改、添加 tcp 及 udp 监听端口等服务。根据组件或软件安装需要，编辑批量安装脚本，开放相应的端口、设置脚本自动安装权限、启动安装服务等。提供软件或组件运性必要的端口修改、添加等服务。 5、初始化服务：提供终端安全管控系统的初始化服务。系统各个组件安装完成后，进行图形管控系统的初始化安装；通过超级管理员或安全审计员账户，实现不同权限控制下的系统管理或安全审计管理。 6、系统初始配置服务：用于完成终端安全管控系统服务器端的初始配置，主要包括组织机构及管理范围、客户端参数配置、客户端安装包发布、扫描范围配置和配置外网地址。（1）组织机构及管理范围配置：配置组织机构及组织机构的 IP 管理范围。（2）客户端注册参数配置：为不同类型的终端配置不同注册界面，显示隐藏功能项，提供更多注册项用于终端注册使用。（3）客户端安装包发布：提供经正式安装测试完全适配濮阳市局国产化终端机型的终端安全		

			加固客户端安装包（zip 压缩包），提供当前市局其它类型终端的客户端安装包，提供客户端升级后的更新包的上载及发布。（4）配置级联地址：提供与部局一级总控级联的地址、端口等参数信息的配置，能够管理本级级联服务的配置信息等。		
		数据迁移服务	在加固版终端安全管控系统部署完成后，针对数据资源、安全策略、资产列表等信息资源进行迁移合并工作，要求新旧终端安全管控系统平台数据迁移期间，迁移工作平滑推进，系统运行正常、保通保活，正常考核。具体迁移服务如下： 1、旧平台服务器信任保护数据向加固版终端安全管控服务器迁移：旧平台服务器上设置信任/保护的设备信息自动同步到加固版终端安全管控服务器资产信息中，内容包括 IP 地址，MAC 地址，设备名称，持有人，所在地，组织机构。 2、通过文件分发策略分发【旧版本终端安全管控系统防火墙卸载程序】进行旧版本客户端的卸载，避免之前存在的卸载旧版本客户端时网卡异常的问题。 3、通过旧版本的软件分发模式分发加固版终端安全管控系统客户端安装包，实现自动更新升级。针对未能分发成功的，可自行注册加固版终端安全管控系统客户端（注册客户端的同时，会自动卸载旧版本客户端）并自动上传注册信息，无需人为干预。 4、备份旧版本终端安全管控系统策略，根据旧版本终端安全管控系统策略要求，在加固版终端安全管控系统服务器上建立对应的策略，并逐步分发。 注意事项：迁移期间，关闭未注册阻断功能；新旧版本终端安全管控系统服务器需要共存一段时间，直到客户端全部迁移到加固版终端安全管控系统服务器，旧版本的服务器至少需要保留三个月。	1	项
		警用地图专题应用	警用地图专题应用能够使计算机终端、警务通移动终端、警车移动终端等信息，在地图上清晰、直观地展现出来，实现数据可视化、地理分析、安全态势分析，达到与已有业务应用的有机集成，实现多维性的需求，主要包括：警务要素上图、车辆轨迹展示、警务信息检索、地址信息采集、基础服务、地图工具和专项应用。	1	项
3	数字证书	国密版公安数字证书	硬件性能规格：1、存储空间≥256K 字节;2、支持 RSA1024、RSA2048、SM2 非对称算法;3、支持 SSF33、SM1 对称算法;4、支持 SHA1、SM3 杂凑算法;5、SM1 算法：512B：≥2.5Mbps，1KB：≥4Mbps，2KB：≥8Mbps，4KB：≥12Mbps，7KB：≥16Mbps;6、SSF33 算法加解密速度≥11Mbps;7、	1000	个

			RSA1024 公私钥对生成一次平均时间≤1.5 秒;8、每秒 RSA1024 签名次数≥20 次;9、每秒 RSA1024 验签次数≥300 次;10、RSA2048 公私钥对生成一次平均时间≤15 秒;11、每秒 RSA2048 签名次数≥30 次;12、每秒 RSA2048 验签次数≥100 次;13、SM2 公私钥对生成一次平均时间≤0.6 秒;14、每秒 SM2 签名次数≥40 次;15、每秒 SM2 验签次数≥25 次;16、SM3 算法性能≥100kbps; 功能要求：1、采用 USB2.0 高速接口，无需附加电源/读卡器，即插即用，简单方便，客户学习成本低。且该产品体积小巧，方便携带，合金材质外壳，坚固轻便；2、支持公安公钥基础设施（PKI）体系，遵循 CSP 和 PKCS11 接口规范设计要求；支持 SM1、SM2、SM3、SM4、SSF33 等国密算法和 RSA1024/2048 等国际算法。提供身份鉴别、数字签名、数据加解密等功能；3、密码算法采用硬件安全芯片实现，严格遵守国家密码管理局提出的“私钥不出芯片”的安全设计理念，确保签名、加解密等操作在安全芯片内部实现。并对敏感数据采用安全存储技术，确保运算的全过程安全可靠；		
4	数字证书适配	公安数字证书国产化终端适配	基于新一代公安数字证书与当前濮阳市局配发的国产化终端适配需要，提供麒麟 V10 操作系统升级服务,支持对麒麟 V10 操作系统进行有关数字证书的补丁包升级，以满足新一代数字证书外设对商密算法的支持，同时支持国产化终端及 X86 客户端的数字身份认证，整体升级适配服务包括：支持在线管理客户端；支持在线自动安装升级包后；支持在线自动安装证书驱动；支持推送公安数字证书驱动客户端。	2000	套
5	数字证书认证网关	公安数字证书安全认证网关	最大新建连接数：≥4000 次/秒；每秒完成交易数（TPS）：≥25000 次/秒；最大并发连接数：≥5500；最大流量：≥850Mbps； 功能参数： 1）动态黑名单功能：系统可以自动更新黑名单、动态更新，不需要重新启动服务；支持 LDAP、HTTP 等多种方式更新；支持 B64、DER 等多种格式； 2）快速检索功能：系统具有快速检索海量数字证书黑名单的功能，可支持百万级黑名单条目数。 3）多站点证书功能：系统可以拥有多个站点证书，不同的服务可以拥有不同的站点证书； 4）多证书链功能：一个 SSL 服务中可同时配置多条证书链，验证不同 CA 的用户证书；	1	套

			5）多种证书支持功能：支持 CFCA、SHECA 及多数省级 CA 中心数字证书； 6）网络应用：支持基于 IP 的所有应用； 7）地址隐藏功能：系统将真正应用服务的地址隐藏，用户仅知道网关地址； 8）支持应用重定向功能：在有防火墙 NAT 映射的情况下正常访问有重定向的网站； 9）认证一致性：系统通过特有的 cookie 技术将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息； 10）自动签名验证：系统自动实现对应用指定数据的签名和验证功能； 11）产品具有《计算机信息系统安全专用产品销售许可证》、《商用密码产品认证证书》；		
6	安全运维终端	安全运维终端	14 英寸 2160*1440，16G 内存，1TB SSD 国产品牌终端，UOS 正版系统	4	台
7	项目运维	项目运维	保证系统平稳运行，降低考核风险、运维风险、保障公安实战业务开展、助力重大活动安保的保通工作以及系统的安全管理、及时升级的业务需要，明确至少 1 名具有终端安全管控原厂服务资质软件工程师提供三年运维服务，持续提供优质的国产化终端及平台可靠运行的维护管理工作。提供针对终端安全管控系统平台的运维服务，包括但不限于巡检服务、考核现场支持服务、应急响应服务、特别时期的现场保通服务、其它任务调度服务、维保总结文档。	3	项

第五部分 合同（样本）

政府采购合同

政府采购合同

采购编号：

需方（全称）：_____

供方（全称）：_____

根据《中华人民共和国民法典》、《中华人民共和国建筑法》及有关法律规定，遵循平等、自愿、公平和诚实信用的原则，同意按照下面的条款和条件订立本政府采购合同，共同信守。

一、政府采购合同文件

本政府采购合同所附下列文件是构成本政府采购合同不可分割的部分：

1.招标文件；

2.招标文件的更正公告、变更公告；

3.中标供应商提交的投标文件、评标现场的质疑答复；

4.政府采购合同条款；

5.中标（成交）通知书；

6.政府采购合同的其它附件。

二、政府采购合同范围和条件

本政府采购合同的范围和条件与上述政府采购合同文件的规

定相一致。

三、政府采购合同标的

本政府采购合同的标的为政府采购合同货物清单(同投标文件中投标产品价格明细表)中所列货物及相关服务。

产品名称	规格、型号	制造厂商	产地	单价	数量	小计
合计　　大写：　　￥：						

四、政府采购合同金额

根据上述政府采购合同文件要求，政府采购合同的总金额为人民币（大写）：　　元（￥：）。

五、产品质量要求及供方对质量负责条件和期限

供方保证所提供的产品是全新（包括零部件）的产品，符合国家检测标准以及该产品的出厂标准（技术、售后服务要求按招标文件及投标文件相应条款制订）。

六、产品调试

产品到达后经验收合格方可安装，安装完毕后供方对产品免费进行安装调试，使其投入正常运行。

七、技术、售后服务要求

按招标文件及投标文件相应条款制订

八、交货时间、地点、方式及完工时间

年　月　日至　年　月　日，供方负责将产品按需方要求在需方指定地点交货、调试完毕，并具备验收使用条件。产品运

送产生的费用由供方负责。

九、付款方式及条件

供方供货、安装、调试完毕，经需方验收格后出具验收报告，向供方支付全部货款。

十、违约责任

1.如果供方未按照政府采购合同规定的要求交付政府采购合同货物和提供服务；或供方在收到需方要求更换有缺陷的货物或部件的通知后10日内或在供方签署货损证明后10日内没有补足或更换货物、或交货仍不符合要求；或供方未能履行政府采购合同规定的任何其它义务时，需方有权向供方发出违约通知书，供方应按照需方选择的下列一种或多种方式承担赔偿责任：

1.1 供方不能交付产品，供方向需方支付未交付部分产品款总值5%的违约金；

1.2 在需方同意延长的期限内交付全部货物、提供服务并承担由此给需方造成的一切损失；

1.3 在需方规定的时间内，用符合政府采购合同规定的规格、质量和性能要求的新零件、部件或货物来更换有缺陷的零件、部件和货物并修补缺陷部分以达到政府采购合同规定的要求，供方应承担由此发生的一切费用和风险。此时，相关货物的质量保修期也应相应延长；

1.4 根据货物低劣程度、损坏程度以及使需方所遭受的损失，经双方商定降低货物的价格或赔偿需方所遭受的损失；

1.5 供方同意退货，并按政府采购合同规定的同种货币将需方所退货物的全部价款退还给需方，并承担由此发生的一切损失和费

用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及需方为保护货物所支出的其它必要费用；

1.6 需方有权部分或全部解除政府采购合同并要求供方赔偿由此造成的损失。此时需方可采取必要的补救措施，相关费用由供方承担。

2.如果供方在收到需方的违约通知书后 10 日内未作答复也没有按照需方选择的方式承担违约责任，则需方有权从尚未支付的政府采购合同价款中扣回索赔金额。如果这些金额不足以补偿，需方有权向供方提出不足部分的赔偿要求。

3.逾期交货的违约责任。

3.1 供方未按政府采购合同规定的交货日期向需方交货时，则每逾期一日，供方应按逾期交付货物价款总值的 1%计算，向需方支付逾期交货违约金，但不超过政府采购合同总金额的 10%。供方支付逾期交货违约金并不免除供方交货的责任。

3.2 如供方在政府采购合同规定的交货日期后 10 天内仍未能交货，则视为供方不能交货，需方有权解除政府采购合同，供方除退还已收取的货款外，还应向需方偿付全部货款 10%的违约金。

3.3 供方所交的产品品种、型号、规格、质量不符合合同规定，需方有权拒收产品，供方应负责更换并承担因更换而支付的实际费用。因更换而造成逾期交货，则按逾期交货处理。

3.4 供方不能按照政府采购合同规定的交付产品，供方向需方支付未交付部分产品款总值 5%的违约金。

4 需方的违约责任：

4.1 需方无正当理由拒收货物、拒付货款的，向供方偿付拒付

部分产品款总额5%的违约金。

5.以上各项交付的违约金并不影响违约方履行政府采购合同的各项义务。

十一、政府采购合同生效

本政府采购合同经双方法定代表人或授权代表签字盖章后生效。

十二、双方约定合同份数：本合同一式 4 份，均具有同等法律效力，供需双方各执 2 份。

其它未尽事宜按照招标文件的规定内容执行。

河南省政府采购合同融资政策告知函

各供应商:

欢迎贵公司参与河南省政府采购活动!

政府采购合同融资是河南省财政厅支持中小微企业发展，针对参与政府采购活动的供应商融资难、融资贵问题推出的一项融资政策。贵公司若成为本次政府采购项目的中标成交供应商，可持政府采购合同向金融机构申请贷款，无需抵押、担保，融资机构将根据《河南省政府采购合同融资工作实施方案》(豫财购（2017）10 号)，按照双方自愿的原则提供便捷、优惠的贷款服务。

贷款渠道和提供贷款的金融机构，可在河南省政府采购网“河南省政府采购合同融资平台”查询联系。

第六部分　附件--谈判文件格式

附件 1

声　明　书

致：河南省濮阳市政府采购中心

_____（供应商名称、地址）授权（代表姓名）_____（职务、职称）为签字代表，参加贵方为采购人采购项目名称　　项目（文件编号：　　）的竞争性谈判采购，并对之负法律责任。

1、声明书

2、濮阳市政府采购供应商信用承诺函

3、报价一览表

4、服务方案

5、资格声明函

6、法定代表人身份证明书

7、法定代表人授权委托书

8、资质证明文件

9、反商业贿赂承诺书

10、中小企业声明函

据此函，法定代表人或被授权人宣布同意如下：

1、所附报价表中规定的应提供和交付的_____项目最低报价为：_____，即（文字表述）_____。

2、如果我们的声明书被接受，我们将履行贵方竞争性谈判文件中规定的每一项要求，按期、按质、按量履行合同。

3、我方愿按《中华人民共和国合同法》履行我方的全部责任。

4、我方已详细审查全部谈判文件，包括修改文件以及全部参考资料和有关附件。

我们完全理解并同意放弃对这方面有不明及误解的权力。

5、我方同意提供按照贵方可能要求的与其谈判有关的一切数据或资料,理解贵方不一定要接受最低报价的谈判或收到的任何谈判文件。

6、本次采购活动有关的一切正式往来请寄：

地址：

邮政编码：

电话：

法定代表人或被授权人（签字或盖章）：

单位名称：（公章）：

日期：

附件 2

濮阳市政府采购供应商信用承诺函

致(采购人或濮阳市政府采购中心):

单位名称:　　统一社会信用代码:

法定代表人:　　联系地址和电话:

我单位自愿参加本次政府采购活动，严格遵守《中华人民共和国政府采购法》及相关法律法规，坚守公开、公平、公正和诚实信用的原则，依法诚信经营，无条件遵守本次政府采购活动的各项规定。我单位郑重承诺，本公司符合《中华人民共和国政府采购法》第二十二条规定的条件:

(一)具有独立承担民事责任的能力;

(二)具有良好的商业信誉和健全的财务会计制度;

(三)具有履行合同所必需的设备和专业技术能力;

(四)有依法缴纳税收和社会保障资金的良好记录;

(五)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;

(六)法律、行政法规规定的其他条件。

我单位保证上述承诺事项的真实性，如有弄虚作假或其他违法违规行为，愿意承担一切法律责任，并承担因此所造成的一切损失。

投标人(企业电子章):

法定代表人或授权代表(签字或电子印章):

日期:　　年　　月　　日

注:　**1.投标人须在投标文件中按此模板提供承诺函，未提供视为未实质性响应招标文件要求，按无效投标处理。**

2.投标人的法定代表人或者授权代表的签字或盖章应真实、有效，如由授权代表签字或盖章的，应提供“法定代表人授权书”。

3.供应商在成交后，应将上述由信用承诺书替代的证明材料提交采购人核验。经核验无误后，由濮阳市政府采购中心发出（成交）通知书。

附件 3

报价一览表

供应商名称：

名称	品牌/型号	生产厂家	单位/数量	单价	总价
。。。。。。。。。					
合计总报价					
备注					

法定代表人或被授权人代表签字：　　单位公章：

日　期：

联系方式：

实质性响应技术条款响应表

序号	名称	招标文件要求技术参数	响应实际参数（响应供应商应按投标/响应货物/服务实际数据填写，不能照抄招标要求）	是否偏离（无偏离/正偏离/负偏离）	偏离简述
1					
2					
3					
4					
5					
6					
7					
8					
…					

注：

1、供应商必须对应采购文件“采购项目技术规格、参数及要求”的内容逐条响应。如有缺漏，缺漏项视同不符合招标要求。

2、供应商响应采购需求应具体、明确，含糊不清、不确切或伪造、变造证明材料的，按照不完全响应或者完全不响应处理。构成提供虚假材料的，移送相关部门查处。

3、本表内容不得擅自删减。

4、**完全**照抄招标文件采购项目技术规格、参数及要求，视为实质性不响应。

供应商法定代表人或授权代表签字或盖章：_____

供应商名称（签章）：_____

日期：　　年　　月　　日

附件 4

服务方案

投标人根据招标文件要求，制定详细服务方案。

附件 5

关于资格的声明函

关于贵方____年____月____日（开标日期）组织的_____竞争性谈判项目（文件编号为）的采购邀请，本签字人愿意参加谈判，并声明提交的下列文件是合法的、有效的。

1、营业执照及项目要求的其他资质证件。

2、法定代表人或被授权人授权书、法定代表人或被授权人身份证。

3、其它证明材料。

本签字人确认资格文件中的说明是合法的、有效的。

单位名称：（公章 ）

法定代表人或被授权人（签字或盖章）：

电话：

地址:

邮政编码：

附件 6

法定代表人身份证明书

法定代表人姓名 在我公司（或企业、单位）任（董事长、经理、厂长）职务，是我（公司全称）的法定代表人。现就参加濮阳市政府采购中心组织的（采购项目名称）（项目编号）的投标签署投标文件。

特此证明。

（※此处法定代表人身份证※）

公司名称：（加盖公章）

年　　月　　日

附件 7

法定代表人授权委托书

委托单位名称：

法定代表人（姓名）：_____

身份证号码：　　住所地：

受委托人（姓名）：_____

身份证号码：

工作单位：　　住所地：

联系方式：办公电话_____　　手机_____

现委托_____为本公司的合法代理人，参加你中心组织的商谈活动。

委托代理权限如下：代为参加并签署_____采购项目名称_____（项目编号_____）的投标文件；代为签订政府采购合同以及处理政府采购合同的执行、完成、服务和保修等相关事宜；代为承认与我公司签署、实施的与采购文件相关的采购活动及行为。

本授权于___年___月___日生效，无转委托，特此声明。

（※此处授权代表人身份证※）

委托单位名称：

年　　月　　日

附件 8

资质证明文件

附件 9

反商业贿赂承诺书

我公司承诺：

在_____项目采购中，我公司保证做到：

一、公平竞争参加本次竞争性谈判采购。

二、杜绝任何形式的商业贿赂行为。不向国家工作人员、政府采购代理机构工作人员、评审专家及其亲属提供礼品礼金、有价证券、购物券、回扣、佣金、咨询费、劳务费、赞助费、宣传费、宴请；不为其报销各种消费凭证，不支付其旅游、娱乐等费用。

三、若出现上述行为，我公司及参与谈判的工作人员愿意接受按照国家法律法规等有关规定给予的处罚。

法定代表人或被授权人（签字或盖章）：

公　章

年　月　日

附件 10

中小企业声明函（货物）

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，提供的货物全部由符合政策要求的中小企业制造。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：

1. *（标的名称）*，属于*（采购文件中明确的所属行业）*行业；制造商为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于*（中型企业、小型企业、微型企业）*；

2. *（标的名称）*，属于*（采购文件中明确的所属行业）*行业；制造商为*（企业名称）*，从业人员_____人，营业收入为_____万元，资产总额为_____万元，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：

***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。**