濮 阳 市 政 府 采 购

文件编号：豫财磋商采购-2023-655

竞争性磋商文件

濮阳市政府采购中心

2023年7月26日

目　　录

第一部分　磋商邀请函

第二部分　磋商项目要求

第三部分　磋商须知

第四部分　竞争性磋商项目内容要求

第五部分　竞争性磋商评分标准

第六部分　合同（文本）

第七部分　附件--商谈文件格式

第一部分 磋商邀请函

一、采购项目：河南省濮阳市中级人民法院信息安全防护设备升级改造项目

二、文件编号：豫财磋商采购-2023-655

三、预算：3020000 元

四、采购需求：见电子招标文件附件

五、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中小企业制造，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。

六、投标人资格及特殊要求：

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 年或 2022 年度经审计的财务审计报告或财务报告（资产负债表、利润表以及现金流量表，公司成立不足一年的从成立之日算起）；

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；

④2023 年 1 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不接受联合体投标

七、是否接受进口产品：否

八、获取招标文件

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、磋商文件的获取、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；

注：首次进入濮阳市公共资源交易平台参加投标的供应商应首先办理以下事项：①办理数字证书：在濮阳市公共资源交易平台(http://www.pyggzy.com/)上查看办事服务-数字证书，准备办证资料，携带数字证书申请表及相关资料前往数字证书受理点办理。 ②详细操作可参考“濮阳市公共资源交易平台(http://www.pyggzy.com/)”办事服务—系统操作指南。

4、售价：无

九、投标保证金：本项目不收取投标保证金。

十、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 8 月 10 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（4））。

3、投标文件递交方式：网上递交。

4、下载招标文件：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台(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、**投标文件递交流程：**供应商登录濮阳市公共资源交易平台(http://www.pyggzy.com/)凭企业数字证书点击“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。

6、**供应商上传的电子加密投标文件，需由供应商按时进入网络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。

7、本次交易项目实行全流程电子化，投标人（供应商）不需到现场参加开标活动。实行网上开标、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，参加网上开标。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（**解密时间为投标截止时间始 30 分钟），**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。

十一、响应文件的开启时间及地点：

1、时间：2023 年 8 月 10 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（4））。

十二、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。

公告期限为五个工作日。

十三、联系方式

1、采购人：河南省濮阳市中级人民法院　　地址：河南省濮阳市开德路 186 号。

联系人：王晓明　　电话：15516633568

采购人负责采购文件的质疑答复

2、采购代理机构：濮阳市政府采购中心

地址：河南省濮阳市中原路和开州路交叉口向北50米路东濮阳市公共资源交易中心一楼北政府采购科。

联系人：黄志锋　　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7月26日

第二部分　磋商项目要求

序号	项　目	内　　容
1	项目名称	河南省濮阳市中级人民法院信息安全防护设备升级改造项目
2	合格投标人的资格条件	详见磋商邀请函
3	供应商要求	参加本次磋商的供应商必须由法定代表人或委托代理人网上参加磋商，并随时接受磋商小组网上询问，并予以解答，否则将拒绝磋商。
4	供货安装时间	合同签订之日起 30 日历天内。
5	履约保证金	不收取
6	服务质量及验收标准	满足国家相关法律规定和现行行业标准与规范和招标文件要求；经检验核实，采购单位按招标文件要求验收合格出具报告。
7	询问和质疑	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。
8	付款方式	本项目所需软硬件设备全部到场且安装调试完成后，支付 50%合同金额，整体项目通过验收合格后支付剩余 50%合同金额。
9	电子投标文件的编制	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，投标文件制作详细操作可参“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）。 2.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。
10	电子标书解密	解密方式：网上解密 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://sj.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招标文件规定时间顺利递交，请供应商事先熟悉网上投标程序。**

第三部分　磋商须知

1、竞争性磋商文件构成。

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

⑴磋商邀请函

⑵磋商项目要求

⑶磋商须知

⑷项目技术要求

⑸合同（文本）

⑹附件--磋商文件格式

⑺反商业贿赂书

2、供应商磋商文件的编写

供应商应仔细阅读竞争性磋商文件的所有内容，按本文件的要求提供磋商文件，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。

4、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）供应商未按规定时间提交磋商文件的。

（2）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。

（3）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。

5、磋商文件的规定

投标文件中凡是要求签署和加盖公章处均须由投标人的法定代表人（负责人）本人或其授权代理人本人签字或盖章并加盖投标人公章。

6、供应商应认真阅读、并充分理解磋商文件的全部内容（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），供应商没有按照磋商文件要求提交全部资料，或者竞争性磋商响应文件没有对磋商文件在各方面都做出实质性响应是供应商的风险，有可能导致其磋商文件被拒绝，或被认定为无效响应或被确定为响应无效。

7、递交磋商文件的密封状态和标记

投标文件按照电子投标的规则密封和标记。

8、磋商文件的递交

（1）电子投标文件递交方式：网上递交。

（2）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。

9、递交磋商文件的截止时间

磋商文件的递交截止时间与磋商开始时间见采购公告。

10、迟交的磋商文件

采购方将拒绝在磋商文件递交截止时间后递交的磋商文件。

11、磋商文件解密

网上解密。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://sj.pyggzy.com/)按时解密。如未在规定时间内解密电子投标文件，其投标将被拒绝。

12、磋商程序

（1）竞争性磋商可以根据项目情况采取多轮磋商，濮阳市政府采购中心在磋商邀请函规定的时间和地点组织网上磋商。

（2）磋商小组对上一轮磋商中所提出的问题与供应商进行下一轮网上磋商，在磋商中磋商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，磋商结束后，磋商小组应当要求所有继续参加磋商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。

（3）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。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，磋商小组应当及时通知所有参加磋商的供应商。

（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内容，并由其法定代表人或分公司负责人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人或分公司负责人授权书。供应商为自然人的，应当由本人签字并附身份证明。

13、磋商小组

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

14、成交原则

（1）磋商小组将遵循公开、公平、公正的原则对待每个参加磋商的供应商。

（2）严格按照竞争性磋商文件的要求，根据质量和服务均能满足采购文件实质性响应要求且最后综合评分最高的原则确定成交供应商。

15、供应商应自行承担所有与参加磋商有关的全部费用。

16、保密及其他注意事项

（1）在磋商期间，供应商不得向磋商小组成员询问其它供应商的磋商情况，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，磋商期间直至授予供应商合同时，磋商小组成员不得与供应商私下交换意见。在磋商结束后，凡与磋商情况有接触的任何人不得将磋商情况扩散出磋商小组成员之外。

（3）不向未成交方解释未成交原因

17、成交通知

磋商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。

18、签定合同

根据成交通知书在约定的时间、地点与需方签定合同。

第四部分 河南省濮阳市中级人民法院信息安全防护设备升级改造项目清单及技术参数要求

信息安全防护设备升级改造项目（中院-专网需求清单）

序号	名称	数量	单位
1	网络安全设备维保升级	3	年
2	终端接入控制系统	1	套
3	潜伏威胁探针	1	套
4	专网终端安全管理系统	1	台
5	服务器	2	台
6	技术支撑服务	2	年
信息安全防护设备升级改造项目（中院-互联网需求清单）			
序号	**产品**	**数量**	**单位**
1	互联网出口下一代防火墙	2	台
2	终端接入控制系统	1	台
3	互联网终端安全管理系统	1	套

清丰县、南乐县两基层法院需求清单

信息安全防护设备升级改造项目（两基层院-专网需求清单）			
序号	**名称**	**数量**	**单位**
1	网络安全设备维保	2	套
2	专网终端安全准入	2	台
3	日志审计	2	台
4	堡垒机	2	台
5	专网终端安全管理系统	2	套
6	等级保护测评服务	2	次
信息安全防护设备升级改造项目（两基层法院-互联网需求清单）			
序号	**名称**	**数量**	**单位**
1	互联网下一代防火墙	4	台
2	终端接入控制系统	2	台
3	互联网终端安全管理系统	2	套

信息安全防护设备升级改造项目（中院-专网、互联网）

技术要求

濮阳市中级人民法院信息安全防护设备升级改造项目（中院-专网）技术要求				
序号	名称	参数要求	数量	单位
1	网络安全设备维保升级	1、针对我院 2020 年采购的网络安全设备，采购设备软件升级授权、安全规则库升级授权等； 2、确保网络安全系统的正常运行。 具体设备如下： a、统一威胁防护 2 台：1）三年软件版本升级；2）三年规则库升级：包括 WEB 应用防护识别库、IPS 特征库、僵尸网络防护库、实时漏洞分析识别库和 URL&应用识别库，保持设备具备检测防御最新威胁的能力。3）三年网关杀毒模块升级许可：包括杀毒模块版本升级、病毒库更新授权。 b、安全网关 2 台：1）三年软件版本升级；2）三年规则库升级：包括 WEB 应用防护识别库、IPS 特征库、僵尸网络防护库、实时漏洞分析识别库和 URL&应用识别库，保持设备具备检测防御最新威胁的能力。3）三年网关杀毒模块升级许可：包括杀毒模块版本升级、病毒库更新授权。 c、统一威胁防护 3 台：1）三年软件版本升级；2）三年规则库升级：包括 WEB 应用防护识别库、IPS 特征库、僵尸网络防护库、实时漏洞分析识别库和 URL&应用识别库，保持设备具备检测防御最新威胁的能力。3）三年网关杀毒模块升级许可：包括杀毒模块版本升级、病毒库更新授权。 d、安全网关 3 台：1）三年软件版本升级；2）三年网关杀毒模块升级许可：包括杀毒模块版本升级、病毒库更新授权。 e、上网行为管理 1 台：1）三年软件版本升级；2）三年 URL&应用识别规则库升级； f、网络安全态势感知系统 1 台：1）三年软件版本升级；2）三年安全感知系统特征库升级，包括：包括安全检测特征识别库、系统更新、文件智能分析模型库、安全知识库、IOC 威胁情报库、热点事件、白名单库等。 g、流量检测探针 1 台：1）三年软件版本升级；2）三年安全感知系统探针特征库升级，包括安全检测特征库系统和威胁情报库升级。 h、终端安全管理系统 1 套：三年软件版本升级包括：（1）产品版本升级；（2）安全云脑在线分析；（3）人工智能算法模型更新；（4）病毒库轻补丁库更新；（5）引擎特征升级等	3	年
2	终端接入控制系统	1、标准机架式设备，高度不低于 1U，标配千兆电口≥6 个，其中支持 ByPass 电口≥1 对，至少支持 1 个扩展槽； 2、产品可适用于 Windows 操作系统及麒麟、统信等操作系统的 PC，具备上网行为审计和终端接入控制（准入）模块，整机吞吐量≥5.8Gb，并发连接数≥50 万，上网行为管理支持用户数≥1000，提供不少于 500 终端接入控制授权； 3、投标人承诺提供整机五年厂家硬件质保、五年系统版本升级、五年全功能模块升级，五年 URL&应用识别规则库升级；	1	套

		★4、支持路由模式、网桥模式、旁路模式部署，支持主主、主备模式部署，支持两台及两台以上设备同时做主机的部署模式，需提供相关功能截图证明； ★5、支持 802.1x 认证，支持对接本地和 AD 域用户源，支持在旁路模式部署下准入生效，需提供相关功能截图证明； 6、支持图形化查看当前局域网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量； 7、支持与本项目所采购的专网终端安全软件联动管理，当检测到终端未安装终端安全软件产品时，禁止上网并提示需要安装终端安全软件； 8、支持接入我院专网安全态势感知平台，实现网络资产信息上报，提升专网整体安全效果； ★9、要求所投产品具备公安部颁发的《计算机信息系统安全专用产品》的销售许可证，许可证内应包含：《网络通讯安全审计类终端接入控制（一级）安全专用产品销售许可证》提供证明材料。		
3	潜伏威胁探针	1、标准机架式设备，高度不低于 1U，网络层吞吐量≥1Gbps，标配千兆电口≥6 个，千兆光口 SFP≥2 个，其中管理口≥1 个，至少支持 1 个扩展槽； 2、投标人承诺提供整机五年厂家硬件质保、五年系统版本升级，五年特征库系统和威胁情报库升级； 3、旁路部署，支持探针接入多个镜像，每个接口相互独立且不影响； 4、支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况。支持通过白流量过滤的方式，过滤安全网站访问，提升性能。 ★5、提供三权分立的用户管理能力：系统管理员、审计管理员、安全管理员、普通管理员四个角色相互独立；普通管理员角色的权限可自定义模块页面的编辑和查看权限，需提供相关功能截图证明； 6、支持基于 IP 和域名的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断，支持 24 小时/7 天/30 天或者自定义时间在 5 分钟内阻断威胁。 ★7、需支持对接我院网络安全态势感知平台，将采集的数据上报至安全分析平台，提升整体安全能力，需提供技术承诺函。	1	套
4	专网终端安全管理系统	1、产品可以纯软件交付，包含管理控制中心软件及终端安全客户端软件，提供不少于 500 套适用于麒麟、统信 PC 终端安全软件授权，并提供五年软件升级授权，包括：产品版本升级，算法模型更新，病毒库、轻补丁库更新，杀毒引擎特征升级等； 2、要求单一管理控制中心，支持同时管控我院现有 Windows 操作系统终端安全软件和麒麟、统信等作系统终端，下发基本安全策略，配置病毒查杀、实时防护、桌面管控等策略，处理终端发生的威胁事件； 3、管理端（控制中心）支持部署环境包括但不限于统信 UOS V20 系统服务器（飞腾 2000、鲲鹏 920）、银河麒麟 V10 系统服务器（飞腾 2000、鲲鹏）、中标麒麟 V7.0 服务器（intel-X86、兆芯）、centos 7+（、intel-X86、兆芯）； 4、终端安全软件客户端支持部署环境包括但不限于：银河麒麟 V4.0（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、中标麒麟 V7.0	1	台

		（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、统信 UOSV20（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、银河麒麟 V10(兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、欧拉、中科红旗、龙蜥等； 5、支持终端自动分组管理，新接入的终端可以根据网段或者关键字自动分配到对应的分组； 6、支持对麒麟、统信等操作系统、芯片厂商、应用软件的资产梳理和统计，帮助运维人员快速且便捷管理麒麟、统信、硬件等相关资产； 1）可直观展示终端替代率、麒麟、统信操作系统版本占比及芯片厂商类型 2）能够基于芯片类型、操作系统类型、终端名称、资产使用人、版本号等多个维度进行终端信息数据筛选及统计； 7、为保障终端数据安全，支持对终端磁盘进行加解密，加解密密钥可在平台统一远控管控；磁盘在脱离管控中断后支持在平台导出密钥使用工具解密； ★8、支持针对分组终端进行违规外联管控，发现违规外联可选择 不处置、断网、关机操作，有效帮助监控内部主机外联行为，及时发现数据泄露风险，需提供相关功能截图证明；； 9、支持对勒索病毒及变种进行防御，可提供勒索病毒基因检测和分析支持；； ★10、支持通过软件定制开发，与我院专网现有的安全态势感知平台进行安全联动，支持管理员在安全感知管理平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，需提供技术承诺函；		
5	服务器（核心产品）	配置 2 颗 10 核心 CPU，内存≥64GB，SSD 硬盘≥480GB，SATA 硬盘≥2TB，双电源。	2	台
6	技术支撑服务	一、技术支撑内容(不少于 2 人，且具有信息安全服务工程师证书） 1、日常安全巡检:主要对机房环境、信息设备的运行状况、设备状态、安全策略进行核查和整改，对涉密重要资产进行核查等。 2、安全审计:主要依据信息系统的安全审计策略，通过对可审计事件、异常事件和行为进行统计分析，形成综合性报告。 3、服务器类维护:主包括服务器操作系统安装、服务器操作系统补丁修补、服务器安全策略配置、服务器可用性监控、服务器可用性分析、服务器日志分析。 4、桌面终端设备类维护:计算机防病毒、安全保密产品安装、BIOS 安全设置、终端硬件故障处理、软件故障处理、软件版本变更、操作系统补丁更新、安全策略配置等。 5、安全保密检查:定期配合保密管理部门进行全面的安全保密检查工作，如终端符合性审查、安全策略符合性审查、安全保密日常核查等。 6、重要业务数据备份恢复:主要包括针对业务系统制定数据备份恢复策略，按照备份策略严格执行数据备份操作。 7、应急响应:是包括安全事件处置响应以及针对各类安全事件制定安全应急预案。至少每年进行一次应急预案培训、应急预案演练、应急预案进行评审和修订。 8、重大事项安全保障:在重要会议、重要审判业务、重大节日期间提供更高级别的安全保障服务。 9、每月利用漏洞检测工具周期性对服务器、网络安全设备等进	2	年

		行全面脆弱性安全检测，有效识别网络、主机等层面的漏洞。 二、威胁分析与处置服务： 1、安全威胁分析：结合安全感知日志和威胁情报进行深度分析，研判网络中存在的威胁和攻击行为，明确对业务的影响和危害； 2、安全事件处置：对安全事件进行处置，清除恶意文件、快速恢复业务； 3、事件溯源分析：深入分析安全事件的成因，发现存在的薄弱点，溯源攻击路径； 4、安全加固建议：根据事件发生的根因、影响范围，针对性给出安全加固方案； 5、按季度审计各类安全事件日志，提交安全加固方案及安全运营效果汇报。 三、安装调试集成服务：包含中院及两个基层法院软硬件安装调试服务（其中包含测试、辅材、运输等相关服务）		
濮阳市中级人民法院信息安全防护设备升级改造项目（中院-互联网）技术要求				
序号	**产品**	**参数要求**	**数量**	**单位**
1	互联网出口下一代防火墙	1、标准机架式设备，高度不低于 1U，标配千兆电口≥8 个，万兆光口≥2 个，其中支持 ByPass 电口≥2 对，至少支持 1 个扩展槽； 2、设备需为专业第二代防火墙产品，配备 FW、应用识别、入侵防御 IPS、防病毒 AV、Web 应用防护模块，整机吞吐量≥20G，应用层吞吐量≥9G，FW+APP+IPS+AV 吞吐量≥1G，HTTP 七层新建连接数≥9 万，IPSec VPN 最大接入数≥1000； 3、投标人承诺提供整机五年厂家硬件质保、五年系统版本升级、五年全功能模块升级、五年规则库、病毒库升级：包括 WEB 应用防护识别库、IPS 特征库、僵尸网络防护库、实时漏洞分析识别库和 URL&应用识别库，保持设备具备检测防御最新威胁的能力； ★4、支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上。需提供相关功能截图证明； ★5、支持对勒索病毒检测与防御功能，可针对勒索病毒攻击设置专项安全策略，需提供相关功能截图证明； 6、产品支持 FTP 协议命令控制功能，至少包含 delete、rmdir、mkdir、rename、mget、dir、mput、get、put 等，保护对外服务不被恶意篡改； ★7、支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁，需提供相关功能截图证明； ★8、产品支持管理员双因子认证，可以通过用户密码和 Key 等不同方式登陆产品管理界面，需提供相关功能截图证明； 9、支持与本项目所采购的终端安全软件联动管理，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置； 10、要求所投产品具备 IT 产品信息安全认证证书 EAL4 增强级，需提供证明材料。	2	台

2	终端接入控制系统	1、标准机架式设备，高度不低于 1U，标配千兆电口≥6 个，其中支持 ByPass 电口≥1 对，至少支持 1 个扩展槽； 2、产品可适用于 Windows 操作系统及麒麟、统信等操作系统的 PC，具备上网行为审计和终端接入控制（准入）模块，整机吞吐量≥3Gb，上网行为管理支持用户数≥500，提供不少于 300 终端接入控制授权； 3、投标人承诺提供整机五年厂家硬件质保、五年系统版本升级、五年全功能模块升级，五年 URL&应用识别规则库升级； ★4、支持路由模式、网桥模式、旁路模式部署，支持主主、主备模式部署，支持两台及两台以上设备同时做主机的部署模式，需提供相关功能截图证明； ★5、网页访问审计支持记录全部或者指定类别 URL、网页标题、网页内容等信息，支持网页内容审计后的网页快照功能；需提供相关功能截图证明； ★6、上网认证支持针对特权用户配置免认证 key、免审计 key、免控制 key，需提供产品截图证明； 7、支持 802.1x 认证，支持对接本地和 AD 域用户源，支持在旁路模式部署下准入生效； 8、支持与本项目所采购的终端安全软件联动管理，当检测到终端未安装终端安全软件产品时，禁止上网并提示需要安装终端安全软件； 9、要求所投产品具备《网络通讯安全审计类终端接入控制（一级）安全专用产品销售许可证》 ，提供证明材料。	1	台
3	互联网 终端安全管理系统	1、产品可以纯软件交付，包含管理控制中心软件及终端安全客户端软件，提供不少于 200 套适用于麒麟、统信 PC 终端安全软件授权，并提供五年软件升级授权，包括：产品版本升级，算法模型更新，病毒库、轻补丁库更新，杀毒引擎特征升级等； 2、要求单一管理控制中心，支持同时管控有 Windows 操作系统终端安全软件和麒麟、统信操作系统终端，下发基本安全策略，配置病毒查杀、实时防护、桌面管控等策略，处理终端发生的威胁事件； 3、管理端（控制中心）支持部署环境包括但不限于统信 UOS V20 系统服务器（飞腾 2000、鲲鹏 920）、银河麒麟 V10 系统服务器（飞腾 2000、鲲鹏）、中标麒麟 V7.0 服务器（intel-X86、兆芯）、centos 7+（、intel-X86、兆芯）； 4、终端安全软件客户端支持部署环境包括但不限于：银河麒麟 V4.0（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、中标麒麟 V7.0（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、统信 UOSV20（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、银河麒麟 V10(兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、欧拉、中科红旗、龙蜥等； 5、支持终端自动分组管理，新接入的终端可以根据网段或者关键字自动分配到对应的分组； 6、支持对麒麟、统信等操作系统、芯片厂商、应用软件的资产梳理和统计，帮助运维人员快速且便捷管理麒麟、统信等相关资产； 1）可直观展示终端替代率、麒麟、统信操作系统版本占比及芯片厂商类型 2）能够基于芯片类型、操作系统类型、终端名称、资产使用人、版本号等多个维度进行终端信息数据筛选及统计；	1	套

		★7、为保障终端数据安全，支持对终端磁盘进行加解密，加解密密钥可在平台统一远控管控；磁盘在脱离管控中断后支持在平台导出密钥使用工具解密，需提供产品截图证明功能有效性； 8、支持针对分组终端进行违规外联管控，发现违规外联可选择不处置、断网、关机操作，有效帮助监控内部主机外联行为，及时发现数据泄露风险 9、支持对勒索病毒及变种进行防御，可提供勒索病毒基因检测和分析支持； ★10、支持与本次所采购的下一代防火墙进行安全联动，管理员在防火墙管理界面下发一键隔离指令，由终端安全软件对终端恶意文件进行隔离，防止病毒进一步扩散，需提供技术承诺函；		

信息安全防护设备升级改造项目（两个基层院-专网、互联网）技术要求

濮阳市中级人民法院信息安全防护设备升级改造项目（基层院-专网）技术要求				
序号	**名称**	**参数要求**	**数量**	**单位**
1	网络安全设备维保	1、针对清丰县、南乐县人民法院 2020 年采购的网络安全设备，采购设备软件升级授权、安全规则库升级授权等三年； 2、确保网络安全系统的正常运行； 具体设备如下： a、统一威胁防护 6 台：1）三年软件版本升级；2）三年网关杀毒模块升级许可：包括杀毒模块版本升级、病毒库更新授权。 b、安全网关 6 台：1）三年软件版本升级；2）三年规则库升级：包括 WEB 应用防护识别库、IPS 特征库、僵尸网络防护库、实时漏洞分析识别库和 URL&应用识别库，保持设备具备检测防御最新威胁的能力。 c、上网行为管理 2 台：1）三年软件版本升级；2）三年 URL&应用识别规则库升级；	2	套
2	专网 终端安全准入	1、标准机架式设备，高度不低于 1U，标配千兆电口≥6 个，其中支持 ByPass 电口≥1 对，至少支持 1 个扩展槽； 2、产品可适用于 Windows 操作系统及麒麟、统信等操作系统的 PC，具备上网行为审计和终端接入控制（准入）模块，整机吞吐量≥3Gb，上网行为管理支持用户数≥500,提供不少于 300 终端接入控制授权； 3、投标人承诺提供整机五年厂家硬件质保、五年系统版本升级、五年全功能模块升级，五年 URL&应用识别规则库升级； 4、支持路由模式、网桥模式、旁路模式部署，支持主主、主备模式部署，支持两台及两台以上设备同时做主机的部署模式，需提供相关功能截图证明； 5、网页访问审计支持记录全部或者指定类别 URL、网页标题、网页内容等信息，支持网页内容审计后的网页快照功能；需提供相关功能截图证明； ★6、上网认证支持针对特权用户配置免认证 key、免审计 key、免控制 key，需提供产品截图证明； 7、支持 802.1x 认证，支持对接本地和 AD 域用户源，支持在旁路模式部署下准入生效； 8、支持与本项目所采购的终端安全软件联动管理，当检测到终端未安装终端安全软件产品时，禁止上网并提示需要安装终端安全软件；	2	台

		9、要求所投产品具备《网络通讯安全审计类终端接入控制（一级）安全专用产品销售许可证》，提供证明材料。		
3	日志审计	1、提供主机审计许可证书数量≥50 个，最大可扩展审计主机许可数≥150，可用存储量≥2TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥2500。 2、标准机架式设备，高度不低于 2U，内存大小≥16G，硬盘容量：≥4T SATA，接口≥6 千兆电口，≥2 个万兆光口。需提供整机五年厂家硬件质保、五年系统版本升级； 3、支持接入 TLS 加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。 ★4、支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。（提供产品界面截图证明）； ★5、支持接入 TLS 加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量（需提供产品界面截图或其他证明材料）。 6、支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等； ★7、支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用（提供产品界面截图证明）； 8、支持预置审计策略模板，包括：Windows 主机类审计策略模板、Linux/Unix 主机类审计策略模板、数据库系统类审计策略模板等； 9、内置主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表等；	2	台
4	堡垒机	1、本次需提供运维授权数≥50，可扩展授权数≥150，图形运维并发数≥100，字符运维并发数≥200。 2、标准机架式设备，高度不低于 1U，硬盘容量：≥2T SATA，接口：≥6 个千兆电口。投标人承诺提供整机五年厂家硬件质保、五年系统版本升级； 3、支持核心资产统一运维管理，账号管理，资产授权，操作行为审计； ★4、全面支持 IPV6，设备自身可以配置 IPV6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登陆和审计（需提供产品功能截图证明）； 5、支持 Windows、linux、麒麟系统、Android、IOS、Mac OS 等客户端操作系统下的 H5 页面一站式运维，实现跨终端适应性 BYOD（Bring Your Own Device）； ★6、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（需提供产品功能截图证明） 7、内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴； ★8、支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批（需提供产品功能截图证明）	2	台

5	专网终端安全管理系统	1、产品可以纯软件交付，包含管理控制中心软件及终端安全客户端软件，提供不少于 250 套适用于麒麟、统信 PC 终端安全软件授权，并提供五年软件升级授权，包括：产品版本升级，算法模型更新，病毒库、轻补丁库更新，杀毒引擎特征升级等； 2、要求单一管理控制中心，支持同时管控现有 Windows 操作系统终端安全软件和麒麟、同学等操作系统终端，下发基本安全策略，配置病毒查杀、实时防护、桌面管控等策略，处理终端发生的威胁事件； 3、管理端（控制中心）支持部署环境包括但不限于统信 UOS V20 系统服务器（飞腾 2000、鲲鹏 920）、银河麒麟 V10 系统服务器（飞腾 2000、鲲鹏）、中标麒麟 V7.0 服务器（intel-X86、兆芯）、centos 7+（、intel-X86、兆芯)； 4、终端安全软件客户端支持部署环境包括但不限于：银河麒麟 V4.0（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、中标麒麟 V7.0（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、统信 UOSV20（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、银河麒麟 V10(兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、欧拉、中科红旗、龙蜥等； 5、支持终端自动分组管理，新接入的终端可以根据网段或者关键字自动分配到对应的分组； 6、支持对麒麟、统信的操作系统、芯片厂商、应用软件的资产梳理和统计，帮助运维人员快速且便捷管理麒麟、统信、硬件等相关资产； 1）可直观展示终端替代率、麒麟统信操作系统版本占比及芯片厂商类型 2）能够基于芯片类型、操作系统类型、终端名称、资产使用人、版本号等多个维度进行终端信息数据筛选及统计； 7、为保障终端数据安全，支持对终端磁盘进行加解密，加解密密钥可在平台统一远控管控；磁盘在脱离管控中断后支持在平台导出密钥使用工具解密； ★8、支持针对分组终端进行违规外联管控，发现违规外联可选择 不处置、断网、关机操作，有效帮助监控内部主机外联行为，及时发现数据泄露风险（需提供产品界面截图或其他证明材料）； 9、支持对勒索病毒及变种进行防御，可提供勒索病毒基因检测和分析支持； ★10、支持通过软件定制开发，与上级单位专网现有的安全态势感知平台进行安全联动，支持管理员在安全感知管理平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，需提供技术承诺函；	2	套
6	等级保护测评服务	基础网络系统的网络信息系统安全等级保护测评服务，并协助单位进行备案，并取得相关证书。	2	次

濮阳市中级人民法院信息安全防护设备升级改造项目（基层院-互联网）技术要求

序号	名称	参数要求	数量	单位
1	互联网下一代防火墙	1、标准机架式设备，高度不低于 1U，标配千兆电口≥8 个，千兆光口≥2 个，其中支持 ByPass 电口≥2 对，至少支持 1 个扩展槽； 2、设备需为专业第二代防火墙产品，配备 FW、应用识别、入侵防御 IPS、防病毒 AV、Web 应用防护模块，整机吞吐量≥4G，应用层吞吐量≥2G，FW+APP+IPS+AV 吞吐量≥450M，并发连接数≥200 万，HTTP 七层新建连接数≥6 万，IPSec VPN 最大接入数≥300； 3、投标人承诺提供整机五年厂家硬件质保、五年系统版本升级、五	4	台

		年全功能模块升级、五年规则库、病毒库升级：包括 WEB 应用防护识别库、IPS 特征库、僵尸网络防护库、实时漏洞分析识别库和 URL&应用识别库，保持设备具备检测防御最新威胁的能力； 4、支持对压缩病毒文件进行检测和拦截，压缩层数支持 15 层及以上。 5、支持对勒索病毒检测与防御功能，可针对勒索病毒攻击设置专项安全策略，需提供相关功能截图证明； 6、产品支持 FTP 协议命令控制功能，至少包含 delete、rmdir、mkdir、rename、mget、dir、mput、get、put 等，保护对外服务不被恶意篡改； ★7、支持服务器漏洞防扫描功能，并对扫描源 IP 进行日志记录和联动封锁，需提供相关功能截图证明； ★8、产品支持管理员双因子认证，可以通过用户密码和 Key 等不同方式登陆产品管理界面，需提供相关功能截图证明； 9、支持与本项目所采购的终端安全软件联动管理，管理员可以在网络防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置； 10、要求所投产品具备 IT 产品信息安全认证证书 EAL4 增强级，需提供证明材料。		
2	终端接入控制系统	1、标准机架式设备，高度不低于 1U，标配千兆电口≥6 个，其中支持 ByPass 电口≥1 对，至少支持 1 个扩展槽； 2、产品可适用于 Windows 操作系统及麒麟、统信等操作系统的 PC，具备上网行为审计和终端接入控制（准入）模块，整机吞吐量≥3Gb，上网行为管理支持用户数≥500，提供不少于 300 终端接入控制授权； 3、投标人承诺提供整机五年厂家硬件质保、五年系统版本升级、五年全功能模块升级，五年 URL&应用识别规则库升级； ★4、支持路由模式、网桥模式、旁路模式部署，支持主主、主备模式部署，支持两台及两台以上设备同时做主机的部署模式，需提供相关功能截图证明； 5、网页访问审计支持记录全部或者指定类别 URL、网页标题、网页内容等信息，支持网页内容审计后的网页快照功能； 6、上网认证支持针对特权用户配置免认证 key、免审计 key、免控制 key； ★7、支持 802.1x 认证，支持对接本地和 AD 域用户源，支持在旁路模式部署下准入生效，需提供产品截图证明； 8、支持与本项目所采购的终端安全软件联动管理，当检测到终端未安装终端安全软件产品时，禁止上网并提示需要安装终端安全软件； 9、要求所投产品具备《网络通讯安全审计类终端接入控制（一级）安全专用产品销售许可证》提供证明材料。	2	台
3	互联网终端安全管理系统	1、产品可以纯软件交付，包含管理控制中心软件及终端安全客户端软件，提供不少于 150 套适用于麒麟、统信 PC 终端安全软件授权，并提供五年软件升级授权，包括：产品版本升级，算法模型更新，病毒库、轻补丁库更新，杀毒引擎特征升级等； 2、要求单一管理控制中心，支持同时管控有 Windows 操作系统终端安全软件和麒麟、统信操作系统终端，下发基本安全策略，配置病毒查杀、实时防护、桌面管控等策略，处理终端发生的威胁事件； 3、管理端（控制中心）支持部署环境包括但不限于统信 UOS V20 系统服务器（飞腾 2000、鲲鹏 920）、银河麒麟 V10 系统服务器（飞腾 2000、鲲鹏）、中标麒麟 V7.0 服务器（intel-X86、兆芯）、centos	2	套

		7+（、intel-X86、兆芯)； 4、终端安全软件客户端支持部署环境包括但不限于：银河麒麟 V4.0（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、中标麒麟 V7.0（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、统信 UOSV20（兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、银河麒麟 V10(兆芯、飞腾 1500/2000、鲲鹏 920、龙芯）、欧拉、中科红旗、龙蜥等； 5、支持终端自动分组管理，新接入的终端可以根据网段或者关键字自动分配到对应的分组； 6、支持对麒麟、统信的操作系统、芯片厂商、应用软件的资产梳理和统计，帮助运维人员快速且便捷管理麒麟、统信相关资产； 1）可直观展示终端替代率、麒麟、统信操作系统版本占比及芯片厂商类型 2）能够基于芯片类型、操作系统类型、终端名称、资产使用人、版本号等多个维度进行终端信息数据筛选及统计； 7、为保障终端数据安全，支持对终端磁盘进行加解密，加解密密钥可在平台统一远控管控；磁盘在脱离管控中断后支持在平台导出密钥使用工具解密； 8、支持针对分组终端进行违规外联管控，发现违规外联可选择 不处置、断网、关机操作，有效帮助监控内部主机外联行为，及时发现数据泄露风险 ★9、支持对勒索病毒及变种进行防御，可提供勒索病毒基因检测和分析支持，需提供产品界面截图或其他证明材料； 10、支持与本次所采购的下一代防火墙进行安全联动，管理员在防火墙管理界面下发一键隔离指令，由终端安全软件对终端恶意文件进行隔离，防止病毒进一步扩散		

第五部分 竞争性磋商评分标准

评分内容	评分细则
报价部分（30分）	有效投标价为不高于采购方预算价限值且通过符合性检查并经磋商后的最终报价： 1、评标基准价的确定：价格得分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格得分按照下列公式计算。 2、投标报价得分=（评标基准价/投标报价）×报价部分权重 30%×100 3、评分计算精确到小数点后 2 位。（四舍五入） 4、若投标报价超出预算控制价，则作为无效标处理。
技术指标项（40分）	参数清单中加★号指标项，为本次采购重要需求指标，投标人所投产品对于性能指标、功能指标需提供包括但不限于产品彩页、产品界面截图、检测报告、相关证书在内的证明材料，每提供一项证明材料得 2 分，满分 40 分；
综合实力（12分）	投标人每提供一份 2020 年以来相关（类似）案例或类似业绩，投标时合同及中标通知书，每提供一份得 1 分，最高得 4 分。
	投标人应具备对信息系统面临的安全威胁、存在的安全隐患进行信息收集、识别、分析和提供防范措施的能力，具备不断的技术更新能力，供应商应具有中国网络安全审查技术与认证中心（CCRC）颁发的信息安全服务资质认证证书-信息系统灾难备份与恢复（B）资质及软件安全开发服务证书，同时具备的得 4 分，提供任意一个的得 2 分，投标时提供证明材料，不提供的不得分。
	所投“专网终端安全管理系统”产品生产厂商具有中国网络安全审查技术与认证中心(CCRC)信息安全服务资质：软件安全开发服务资质认证证书，具备软件安全开发一级服务资质得 4 分，软件安全开发二级服务资质得 2 分（软件安全开发服务资质不重复计分），投标时提供证明材料，否则不得分。
项目实施及售后（18分）	1、投标人针对本项目编制的实施方案情况进行打分： 内容包含但不限于：①实施整体规划；②供货方案；③调试方案；④验收方案；⑤应急预案；优秀得 5 分，合理的得 3 分，较差的得 1 分。 2、投标人提供培训方案情况： 投标人提供详细具体的培训方案，全面、详细、合理、切实可行的得 5 分，较完整的得 3 分，一般的得 1 分 3、在满足招标人的服务要求及标准前提下，比较各投标人提交的售后服务方案，根

	据售后服务方案进行打分，售后服务内容，方式详尽的程度，流程明朗清晰程度（0-5分）。 优：得5分；良：得3分；一般：得1分。 （0-5分）未提供不得分 4、对本项目的合理化建议，及对在质保期内、质保期外的服务计划、承诺等有其他实质性优惠被磋商小组认可1项得1分，共3分。

第六部分 政府采购合同模板

供方：

需方：

供需双方根据　　年　　月　　日河南省濮阳市政府采购中心签发的招标采购中标通知书和招投标文件，并经双方协商一致，达成以下合同条款：

一、项目名称、品牌型号、数量及金额。

二、质量要求、售后服务、质保期。

供方提供的货物须符合国家相关标准及该产品的标准（要求、售后服务等要求按招标文件及投标文件相应条款执行）。

售后服务：　。

质保期：　。

三、交货时间、地点、方式：

　　年　　月　　日至　　年　　月　　日，供方负责将货物按需方要求在交货，并负责调试安装，达到国家相关验收标准，运送货物所产生的费用由供方负责。

四、付款方式：见招标文件

五、违约责任：

需方无正当理由拒收货物、拒付货款，向供方偿付、拒付货物款总额5%的违约金。

需方逾期付货款，向供方每日偿付欠款总额1%的违约金。

供方所供的货物品种、质量不符合合同规定，需方有权拒收货物，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。

供方不能交付货物，供方向需方支付货物款总值10%的违约金。

供方逾期交付货物，供方向需方每日偿付逾期货物款总值1%的违约金。

六、合同签定后，需方不承担涉及专利权、商标权、著作权和外观设计权等侵权责任，因侵权而引起的纠纷或赔偿均由成交方承担。

七、因货物的质量问题发生争议，由法定的质量技术监督部门进行质量鉴定，

该鉴定结论是终局鉴定，供需双方均应当接受。

八、本合同发生争议产生的诉讼，由合同签订所在地人民法院管辖。

九、合同生效及其它：

本合同经双方代表签字并加盖公章后生效。本合同一式___份，_____

供方：	需方：
地址：	地址：
法定代表人：	法定代表人：
委托代理人：	委托代理人：
联系电话：	联系电话：
开户银行：	
帐号：	
	签订时间：
	签订地点：

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。

第七部分　　附件--磋商文件格式

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：　　）的竞争性磋商采购，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、其它证明文件

10、反商业贿赂承诺书

11、中小企业声明函

12、联合体协议

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（人民币大写）_____。

2、如果我们的声明书被接受，我们将履行贵方竞争性磋商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磋商文件，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磋商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磋商或收到的任何磋商文件。

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

详细服务方案

1、投标人根据技术服务要求及评分标准，制定详细服务方案.

2、并承诺以下服务要求：本次项目招标包含中院及两个县区法院的专网、互联网的整体安全加固防护，要求整体项目提供三年免费的售后服务。

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_____竞争性磋商项目（文件编号为）的采购邀请，本签字人愿意参加磋商，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、法定代表人身份证或法定代表人授权书、法定代表人授权代表身份证。

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复印件※）

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

其他证明文件

附件 10

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磋商采购。

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，我公司及参与磋商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 11

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：

备注：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。

2、依据财政部、工业和信息化部制定财库〔2020〕46 号《政府采购促进中小企业发展管理办法》规定，不符合或非小型、微型企业生产货物投标时不用提供该声明。