襄阳市第一人民医院
XIANG YANG NO.1 PEOPLESHOSPITAL
湖北医药学院附属襄阳市第一人民医院
AFFILIATED HOSPITAL OF HUBEI UNIVERSITY OF MEDICNE

襄阳市第一人民医院

院内采购文件

采购方式： ☑磋商；☐谈判；☐询价； ☐需求调查（市场调研、价格摸底）；☐其他：_____

项目类型： ☐工程；☐货物； ☑服务；☐其他：_____

需求部门： 信息中心

项目名称： 2025 年度线上未知威胁监测处置服务项目

项目编号：

采购日期： 年 月 日

其他：

目 录

第一章 采购公告（采购邀请函）

襄阳市第一人民医院拟对如下项目进行采购，欢迎符合条件且诚意合作的供应商踊跃投标。

一、项目概述

（一）项目编码：XYYY-2025-YNCS-0145

（二）项目名称：2025 年度线上未知威胁监测处置服务项目

（三）项目概述：

1. 拟采购一套外部业务网络安全监测处置服务。

2.合同履约期限：1 年。

（四）项目预算总金额：29.8 万元

二、申请人资格要求

(一)满足《中华人民共和国政府采购法》第二十二条规定，即：（1）具有独立承担民事责任的能力；（2）具有良好的商业信誉和健全的财务会计制度；（3）具有履行合同所必需的设备和专业技术能力；（4）有依法缴纳税收和社会保障资金的良好记录；（5）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；（6）法律、行政法规规定的其他条件。

（二）单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加本项目同一合同项下的采购活动。

（三）本项目不接受联合体投标，投标人中标后不允许分包。

（四）通过“信用中国”网站或者中国政府采购网查询的主体信用记录，未被列入信用失信被执行人、重大税收违法案件当事人名单，未被列入政府采购严重违法失信行为记录名单。

（五）本项目特定资格要求：投标人或其代理厂商需具备由中国信息安全测评中心评估的“安全运营类一级”能力认证。（提供中国信息安全测评中心官网查询截图并加盖原厂公章）

（六）报名时需要提供的资料具体详见附件 3。

三、报名时间和地点

（一）报名时间：2025 年 9 月 23 日 8 时至 2025 年 10 月 11 日 17 时 30 分。

（二）报名地点：襄阳市第一人民医院招标采购办（沿江大道江边住院大楼对面行政楼 106)工作日上午 8:00～12:00、下午 14:30～17:30 受理投标工作，节假日除外）。

四、采购会议时间：以招标采购办电话通知时间为准。

五、采购文件获取

投标人在襄阳市第一人民医院官网（https://www.xysdyrmyygw.com）招标公告—招标信息栏**自行下载采购文件**。

六、报名要求

供应商报名应提供的证明材料**（全部资料均需加盖公司原章，否则视为无效）**

（一）法人身份证明或法定代表人授权委托书（请严格按照附件格式出具法人和受托人的身份证复印件）

（二）营业执照

（三）按照“申请人资格要求”中提供相关证明材料。

（四）公司承诺书（对本公司提供报名资料复印件真实性的承诺）。

七、其他

（一）供应商在接到会议通知后将投标文件密封，并按要求准备好标书五份（一正四副），将正本和所有的副本、电子文档密封，并进行包封。包装封皮上均应注明项目名称、项目编号、包号、供应商名称，加盖供应商单位公章。如果投标人未按上述要求密封，其投标文件将被拒绝接收。

（二）参与投标时需具有法定代表人或其他组织或自然人等资格证明文件，法定代表人或其他组织或自然人不能亲自投标的，可以授权他人进行投标，需提供授权委托书，项目受托人身份证原件等各类资料证件。**（供应商根据自身情况提供对应的证明材料，此项资料除**

了投标文件中需提供外，额外放一份在密封完好的投标文件外面，投标时用于核对身份）。

（三）若采购会议前更换受托人，新受托人需携带新的法人授权委托书和相关资料到现场。采购文件中若要求提供样品，则供应商必须携带样品入场，否则视为自动弃权。

（四）诚信履约：已报名供应商若主动放弃参与，必须在**项目开标前提前3个工作日电话告知招标采购办，同时至少提前1个工作日将弃权声明报送至采购办，否则，将会被列入我院失信供应商名单，**直接影响后续各项目的参与。

（五）供应商应仔细阅读招标文件的所有内容，按招标文件的要求提供完整的投标文件，并保证所提供的全部资料的真实性，以使其投标对招标文件作出实质性响应，否则其投标可能被拒绝。如投标人只对部分要求作出响应或书写不清，给评标造成困难的，责任由投标方承担。

八、联系方式

报名联系电话：招标采购办公室0710-3420737

九、发布公告媒介

本次公告仅在襄阳市第一人民医院(https://www.xysdyrmyygw.com)网上发布，信息以本网站发布为准。

第二章　供应商须知

供应商应严格按照本须知要求进行响应，否则采购人有权否决

序号	条款名称	编列内容
1.	采购人	襄阳市第一人民医院
2.	供应商	资格要求：符合本文件公告规定
3.	响应文件装订要求	必须提供装订成册一式五套的响应文件（含一正四副），将正本和所有的副本、电子文档（**U盘，需包含已盖章文件扫描件**）密封，并进行包封。包装封皮上均应注明项目名称、项目编号、包号、供应商名称，加盖供应商单位公章。
4.	响应文件编列要求	见响应文件格式，格式中有具体要求的，供应商必须响应，否则可能导致响应文件被拒绝。
5.	响应文件有效期	不少于90日历天
6.	样品	□提交；　☑不提交；　样品要求：
7.	采购方式	（1）询价：供应商按要求一次报出不得更改的价格，采购人从询价小组提出的成交候选人中，根据质量和服务均能满足采购文件实质性响应要求且报价最低的原则确定成交供应商的采购方式。 （2）谈判：供应商按照谈判文件的要求提交响应文件和最后报价，采购人从谈判小组提出的成交候选人中，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报价最低的原则确定成交供应商的采购方式。 （3）磋商：供应商按照磋商文件的要求提交响应文件和报价，采购人从磋商小组评审后提出的候选供应商名单中，根据评分按照排序由高到低的原则确定成交供应商 （4）需求调查（市场调研、价格摸底）：采购人面向市场主体开展需求调查，以了解实现项目目标，拟采购的标的及其需要满足的技术、商务要求。 （5）其他：需采用其他方式采购的项目，另行说明
8.	项目类型	货物：是指各种形态和种类的物品，包括原材料、燃料、设备、产品等。 工程：是指建设工程，包括建筑物和构筑物的新建、改建、扩建、装修、拆除、修缮等。 服务：是指除货物和工程以外的其他采购对象。
9.	定标办法	☑综合评价；　□最低价；□其他：
10.	签字盖章要求	供应商应在所有格式要求应加盖公章处加盖供应商单位公章，在所有格式要求应加盖法定代表人章或法定代表人签字处加盖法定代表人章或签字。
11.	解释权	本采购文件解释权归襄阳市第一人民医院所有
12.	合同授予	本文件不作为合同授予的唯一依据
13.	诚信履约	已报名供应商若主动放弃参与，必须在项目开标前提前3个工作日电话告知招标采购办，同时至少提前1个工作日将弃权声明报送至招标采购办，否则，将会被列入我院失信供应商名单，直接影响后续各项目的参与。采购人有权将具有弄虚作假、无故拒绝履约、不签订合同、串通投标、围标等情形的供应商将按医院《襄阳市第一人民医院招标采购供应商黑名单

		管理办法》有关要求执行。

注：表格中“☑”

第三章 采购需求

（一）采购内容

序号	采购内容	单位	数量	技术要求
1	外部攻击面专家监测服务	套	1	详见第二部分
2	全时段未知威胁托管检测响应服务	套	1	
3	全资产安全事件托管监测服务	套	1	
4	网站安全监测服务	套	1	

（二）技术功能要求

序号	指标项	指标要求
一、外部攻击面专家监测服务		
1	资产范围	(1) 支持针对采购方 50 个 IP/子域名、5 个根域名、50 个关键字以攻击者视角进行外部攻击面监测，并针对医院的攻击暴露面、影响面情况与改进建议进行专业化分析总结，服务周期 1 年。
2	暴露面检测	(2) 资产探测：服务支持基于资产探测任务的结果，深度识别并记录资产下各种资产属性，包含但不限于：子域名、IP、开放端口服务应用、资产变动情况、HTTP 响应码、端口 banner、组件、归属地、SSL 证书。
		(3) 关键字监控：服务支持根据采购方定义的特定关键字或关键字组合，发现并监测微信公众号、微信服务号、微信小程序、APP 的资产及变化情况；支持识别资产内容包括但不限于：账号主体、资产类型、微信号、简介。
		(4) 影子资产识别：投标人支持通过将客户域名、组织名称、备案号、业务关键字等属性与全球互联网资产进行关联匹配，对医院互联网资产进行测绘，并辅助医院确认归属，以发现“影子资产”。
		(5) ▲暴露面可视化：投标人提供专业的可视化管理页面，方便采购方进行暴露面管理，管理页面可以呈现相应 IP/域名的风险等级、风险数量、责任部门，并展示相应 IP/域名的端口、服务、WEB 状态码、指纹、访问路径、是否影子资产等信息。（提供暴露面管理界面截图，展示以上可呈现的基本信息，并加盖原厂公章）
3	攻击面分析	(6) 攻击视角漏洞检测：服务支持基于指纹从网络侧发起主动扫描识别漏洞，漏洞类型包括但不限于：Web/应用漏洞、中间件/常用软件漏洞、数据库漏洞、系统漏洞、云类型（容器、虚拟化、云原生等）、设备型漏洞。

		(7) ▲攻击面漏洞分析：服务支持基于暴露面检测的结果，针对互联网资产进行 PoC 漏洞扫描，PoC 漏洞类型包含但不限于：未授权访问漏洞、数据库弱口令、远程登录协议弱口令、远程代码执行漏洞、SQL 注入、敏感信息泄露漏洞、文件上传漏洞等。（提供漏洞风险管理界面截图并加盖原厂公章，证明能展示漏洞名称、漏洞 URL、漏洞类型、风险等级、CVE ID、端口、跟进状态等）
		(8) 弱口令识别：服务支持识别 FTP、IMAP、MSSQL、MySQL、ORACLE、PCAnywhere、POP3、SMB、SMTP、Telnet、SSH、RDP、rsync、WMI、WinRM、Exchange、Redis、Mongodb、PostgreSQL、LDAP、SVN、Tomcat、WebLogic、SNMP、Activemq 等超过 25 种协议/服务的弱口令。（提供弱密码管理界面截图并加盖原厂公章，证明能够展示资产弱密码所涉及的账号、端口、类型、发现时间及跟进状态）
4	敏感数据泄露监测	(9) ▲泄露风险监测：投标人能够根据采购人定义的关键字或关键字组合，对 Telegram 等黑客活跃的即时通讯软件、互联网网盘的共享文档、互联网文库的共享文档、GitHub/Gitee 等国内外主要开源社区/代码托管平台、暗网中的交易平台、黑客地下论坛、勒索团伙站点、窃密团伙等进行监测并保持记录，分析发现采购人相关的敏感文件泄露事件。（提供数据泄露监控的界面截图并加盖原厂公章，证明展示数据泄漏事件的风险等级、类型、IP 标签及事件描述）
		(10) 商誉风险监测：服务能够检测并识别采购人外部视角开放的业务所面临的商誉风险，如 SSL 证书临期、网站断网等商誉风险事件。（提供承诺函）
二、全时段未知威胁托管检测响应服务		
1	资产范围	(11) 为采购人至少 20 个资产提供 7*24 小时的全时段未知威胁托管检测响应服务，服务周期 1 年。
2	服务平台	(12) ▲服务平台能力保障：服务的云端服务平台应通过国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部四部委联合组织的云计算服务安全评估，入选“通过云计算服务安全评估的云平台”名单，以确保平台的安全性和可控水平。（提供中央网络安全和信息化委员会办公室、国家互联网信息办公室官方网站发布的《通过云计算服务安全评估的云平台》入选名单截图并加盖原厂公章）
		(13) ▲服务平台安全合规：服务的云端服务平台应当做好严格的安全防护，并严格按照《信息安全技术—网络安全等级保护基本要求》完成等级保护测评工作，服务平台至少通过等级保护三级测评。（提供安全运营中心/安全运营平台等级保护三级测评结果证书截

		图并加盖原厂公章）
3	AI 能力集成	(14) ▲服务基于 AI 技术、多级安全专家的分层能力，满足采购人安全服务效果的实时性、精准性、专业性，实现精准告警、动态响应的安全保障能力。（提供安全服务平台的官网介绍界面截图并加盖原厂公章，证明安全服务的AI 能力集成及安全专家分级响应能力）
4	7*24H 专家服务	(15) ▲应当具备云端检测和分析平台，通过采集采购人安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，同时配备专属管家，为采购人提供 7*24 小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示。（提供服务平台 7*24 小时服务管家展示截图并加盖原厂公章，能够展示管家处置事件、处置威胁的具体数量情况）
5	威胁研判	(16) ▲服务支持针对采购人网络内存在的已知/未知安全威胁进行分析研判，呈现威胁的类型、威胁等级、影响资产、发生时间与闭环时间，并且明确展示威胁的响应时长和闭环时长，在威胁详情中能直观展示出威胁的基础信息、威胁描述及处置建议，并呈现服务专家威胁发现、审核、跟踪处置、完成闭环的时间节点流程，（提供服务平台威胁管理看板及具体威胁的处置流程界面截图并加盖原厂公章，需要包含上述威胁研判相关要素）
6	事件管理	(17) ▲服务支持全流程的安全事件生命周期管理，包括但不限于勒索病毒、反序列化攻击、Webshell 通信、远程代码执行、暴力破解、漏洞利用、SQL 注入、僵尸网络、隐秘隧道、WANNACRY、永恒之蓝、恶意脚本、异常外联、挖矿病毒、蠕虫病毒、后门软件、下载恶意文件等安全事件，能够展示安全事件的类型、影响主机 IP、事件描述与处置建议，并呈现安全事件有服务专家发现、研判审核、跟踪处置与闭环的具体流程时间节点。（提供服务平台事件管理看板及具体事件的处置流程界面截图并加盖原厂公章，需要包含上述事件研判相关要素）

7	服务SLA承诺	(18) ▲为了降低采购人因网络安全事件造成的损失和影响，安全服务团队应当按照以下服务指标和要求为采购人提供服务： 1) 从安全日志产生到事件通告给采购人的时间方面，按照国家标准对安全事件的分类分级指南，重大安全事件通告时间小于30分钟，一般事件的通告时间少于1小时； 2) 在配备投标人的边界防护服务组件和终端防护服务组件的情况下，高级威胁的处置完成时间少于1小时，一般威胁的处置完成时间少于4小时； 3) 安全事件经过服务人员的确认后，通告给采购人的各类安全事件的准确率不低于99%（即误报不能超过1%）； 4) 投标人应当承诺，服务范围内的所有安全事件的闭环处置比例达到100%。 5) 投标人应当满足重大事故应启动应急响应机制，工作时间15分钟之内云端专家进行响应，非工作时间30分钟之内云端专家进行响应，省会2小时上门处置，省内8小时上门处置。 （提供关于以上SLA指标的承诺书并加盖原厂公章）
8	服务交付物	(19) ▲投标人需为采购人提供的服务成果展示门户，可以直观的管理服务过程中生产的服务报告和交付物，包括但不限于《准备阶段文件》、《特殊时期值守报告》、《运营月报》、《威胁情报》、《年度汇报》、《事件总结报告》。（提供关于以上报告管理的可视化服务平台界面截图并加盖原厂公章）
三、全资产安全事件托管监测服务		
1	资产范围	(20) 为采购人至少500个资产提供工作日5*8小时的专家安全事件托管监测服务，服务周期1年，服务内容包括安全事件分析研判、安全事件告警、安全专家协助处置及安全报告，服务周期内按采购人需求提供不低于9次一般安全事件的专家处置协助（并输出事件处置报告）及2次重大安全事件应急响应服务（并输出应急响应报告）。
2	安全事件分析与研判	(21) 安全服务专家支持对平台接入采购人安全组件后所生成的安全事件进行分析研判，包括但不限于确认主机是否感染恶意病毒木马，黑客攻击状态是否成功等，并且保障安全事件准确率不低于99.9%。
3	安全事件告警	(22) 安全服务专家将分析研判后确定的安全事件结果同步到用户的平台，同时安全专家每日对分析研判的各类安全事件进行总结并向用户发送每日总结快报。

4	一般事件处置	(23) 安全服务专家工作日 5*8 小时在线，响应用户发起的协助处置工单，帮助用户对资产内的一般事件（如病毒木马、挖矿病毒、恶意攻击等）进行远程处置，输出《事件处置报告》。
5	重大事件响应	(24) 安全服务专家在线 5*8H 在线响应，响应用户发起的应急工单，协助用户对网络内发生的重大安全事件进行处置，包括对事件进行紧急遏制、检测和分析事件的影响范围、开展事件的溯源调查、提供响应后的安全加固方案，输出《应急响应报告》。
6	服务平台	(25) ▲全资产安全事件托管监测服务与全时段未知威胁托管检测响应服务平台保持一致，支持在同一平台用户管理界面展示 5*8H 及 7*24H 托管信息化资产的安全威胁研判情况、事件管理情况、威胁与事件相应处置流程情况。（提供服务平台威胁管理与事件管理界面截图并加盖原厂公章，展示明确的服务资产 5*8、7*24 标签及 5*8H 服务的服务工单情况）
四、网站安全监测服务		
1	资产范围	(26) 为采购人提供至少 20 个二级域名网站提供网站安全监测服务，监测范围包括关键字敏感信息监测、网页黑链篡改监测、网页挂马监测、网站可用性监测。
2	篡改监测	(27) 支持持续对目标站点主要页面进行监测，精准匹配敏感信息，发现网页敏感词事件第一时间主动通知采购人，监测内容记录在报告中。
		(28) 支持对目标站点的网页黑链篡改、网页挂马进行监测，发现后提供安全专家人工验证。
		(29) ▲支持对目标站点进行实时篡改监测，首页每 5 分钟一次，全站每 3 天一次，一旦发现被篡改第一时间对采购人进行告警。（提供监测服务承诺函并加盖原厂公章）
3	可用性监测	(30) ▲支持自动持续对网站的可用性进行探测，网站的首页 url 保持每 10 分钟探测一次，及时发现断网故障，主动告警通知采购人。（提供监测服务承诺函并加盖原厂公章）
		(31) 支持多节点的可用性探测，提供的监测节点不少于 3 个，各节点的分布地点需位于不同城市。

（三）综合要求

1．服务期：3 年，本期为第一期，评估无违约可续签一年，最多续签两年。

2．服务：供应商在服务期内需提供1名驻场人员，驻场人员需具备网络安全相关的认证证书。

3．付款条件及方式：项目验收后付首笔款。

第四章　评定办法

一、初步评审：

审查内容		评审因素
初步评审	具有独立承担民事责任的能力	供应商具有有效的营业执照或事业单位法人证书或社会团体法人登记证书或执业许可证或自然人身份证明等证明文件（供应商根据自身情况提供对应的证明材料）。
	具有良好的商业信誉和健全的财务会计制度	（1）法人：提供本年度（或上一年度）经第三方审计的财务报告（完整的财务报告，包括“四表一注”，即资产负债表、利润表、现金流量表、所有者权益变动表及其附注）或其基本开户银行出具的资信证明；），或银行资信证明。 （2）部分其他组织和自然人：没有经第三方审计的财务报告的，可以提供银行出具的资信证明； （3）投标人没有经第三方审计的财务报告和资信证明时，也可以提供财政部门认可的政府采购专业担保机构出具的投标担保函。
	具有履行合同所必需的设备和专业技术能力	由供应商提供书面承诺或证明，或提供相应证明材料。
	有依法缴纳税收和社会保障资金的良好记录	（1）供应商应依法缴纳税收：本项目公告发布时间前 12 个月内（至少有 1 个月）缴纳税收的凭据（完税证、缴款书、印花税票、银行代扣（代缴）转账凭证等均可）。 （2）供应商应依法缴纳社会保障资金：本项目公告发布时间前 12 个月内（至少有 1 个月）缴纳社会保险的凭据（专用收据或社会保险交纳清单）。 （3）提供投标企业与被授权人签订的劳动合同和投标企业为被授权人缴纳社保金的证明材料。
	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	政府采购法第二十二条第一款第五项所称重大违法记录，是指投标人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；（提供承诺书，格式详见响应文件格式）。
	法律、行政法规规定的其他条件	（供应商主动自行提供）国家对生产和销售相关产品或提供相关服务有专门法律、行政法规规定的，国家法律法规对市场准入有要求的还应提交相关资格证明文件。
	禁止参加情况	(1)单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加本项目同一合同项下的政府采购活动。 (2)为本采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的，不得再参加本项目的其他招标采购活动。（提供承诺，见响应文件格式）
	主体信用记录	本项目公告发布后，参加本次采购活动前，通过“信用中国”网站（www.creditchina.gov.cn）或中国政府采购网（www.ccgp.gov.cn）查询失信被执行人、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。
	联合体	本项目不接受联合体投标，投标人中标后不允许分包

	特定资格条件	符合本文件第一章第二款第（五）条本项目特定资格要求
	投标人名称	与营业执照等其他证件一致
	签字盖章	有法定代表人或其委托代理人签字并加盖单位公章
	投标人身份证明文件	具有法定代表人或其他组织或自然人等资格证明或法定代表人授权委托书
	投标报价	每一种采购内容只有一个报价；是否按照采购文件的报价要求进行报价，投标报价合理；
	采购需求	*号条款（如有）是否符合采购文件要求；是否实质性响应采购文件；
	其他要求	符合法律、法规和采购文件中规定的其他实质性内容的

二、详细评分办法（详细评分表）

评分要素	评分项	分值	评分标准
价格部分（15 分）	投标报价	15	以通过资格性审查符合性审查，实质性响应采购文件要求且报价最低的响应报价为评审基准价（须未超过采购预算或最高限价（如有），其价格分为满分 15 分。其他投标人的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）×价格权值×100（价格权值为 15%）
技术部分（47 分）	技术要求	35	投标文件第三章中第二部分中功能要求全部满足招标要求的得 35 分。标注“▲”号的功能指标，每不满足一项扣 2 分，未标注“▲”号的功能指标，每不满足一项扣 1 分，扣完 35 分为止。根据投标单位磋商响应文件中提供的偏离表（需要证明材料的提供相应承诺函或者证书，未标明证明材料形式的以偏离表中应答为准）是否满足进行评分。未按要求制作偏离表及证明材料的不得分。如果在本次投标中标注无偏离和正偏离的内容在中标后未予实现，我院可单方面终止合同，同时乙方需无条件赔付合同金额 200%的违约金给我院。
	项目需求设计分析	10	投标人充分了解采购人的安全服务需求，并根据采购人实际安全问题进行分析梳理，输出采购人网络安全态势、网络安全现状及需求，匹配安全服务总体建设框架，并提供所供应安全服务的专业技术白皮书。 1.需求分析完善、贴合实际，方案框架合理，技术白皮书标准、完整的得 7-10 分； 2.需求分析完整、有可行性，部分符合项目需求的得 4-6 分； 3.分析内容不全面，有缺陷的得 1-3 分； 4.不满足院方要求或未提供方案的，得 0 分。

	服务接入	2	为保障安全服务的数据采集与分析标准化，保障服务效果，本次所投安全服务支持对接采购人现网的态势感知平台、防火墙及主机安全防护系统等安全设备，通过安全、稳定、实时的数据采集与分析能力，能实时、有效地检测采购人现网的网络安全问题并提供响应服务。提供安全服务与现网安全设备的对接承诺函及对接显示界面截图并加盖原厂公章的得 2 分。
商务部分（38 分）	投标人能力认证	10	投标人自身具有 CCRC 信息系统安全集成服务资质得 2 分,不具备不得分。证明文件需提供证书复印件，并加盖投标人公章。
			投标人自身具有 CCRC 信息系统安全运维服务资质得 2 分,不具备不得分。证明文件需提供证书复印件，并加盖投标人公章。
			投标人自身具有《ISO9001 质量管理体系认证证书》得 1 分,不具备不得分。证明文件需提供证书复印件，并加盖投标人公章。
			投标人自身具有《ISO27001 信息安全管理体系认证证书》得 1 分,不具备不得分。证明文件需提供证书复印件，并加盖投标人公章。
			投标人自身具有《ISO20000 信息服务管理体系认证证书》得 1 分,不具备不得分。证明文件需提供证书复印件，并加盖投标人公章。
			投标人自身需有一定的服务能力为本次服务项目提供专业的服务团队支撑，团队人员具备 CISP 资质认证证书、安全服务厂商认证的安全资深工程师认证证书和云计算资深工程师认证证书。 以上每满足一项得 1 分，不具备不得分，满分 3 分。提供人员社保信息及资质证书复件材料并加盖投标人公章。
	类似业绩	10	投标人需提供自主取得的自 2020 年 1 月 1 日至今的网络安全服务业绩案例，每有一项有效业绩得 1 分。 注：以合同签订时间为准，需提供项目合同关键页复印件（至少包括封面页、服务内容页、合同签字页、验收报告等四项内容）并加盖公章。

	安全服务提供商技术能力	4	云计算应用服务能力：采购人各项业务通过云计算底座进行承载，针对云业务及云业务应用数据的安全服务保障效果应当得到保障。 投标人或其代理厂商具备由中国信息安全测评中心认证的“云计算安全类一级”、“数据安全类一级”能力。 提供中国信息安全测评中心官网查询截图并加盖原厂公章，每满足1项的得2分。
		4	漏洞安全检测与保护能力：为保障服务团队在漏洞情报层面的专业能力，投标人或其代理厂商为国家信息安全漏洞共享平台(CNVD)技术组、国家信息安全漏洞共享平台(CNVD)用户组成员，每满足一项得2分，提供网站链接与截图证明并加盖原厂公章。
		5	安全事件应急响应能力：为保障服务团队的安全应急响应能力，投标人或其代理厂商入选国家互联网应急响应中心网络安全应急服务国家级支撑单位，近五届中，每入选一届得1分，满分5分，提供国家互联网应急响应中心官网截图并加盖原厂公章。
	项目技术团队	5	投标人或其代理厂商需具备国际范围的安全服务运营中心专家团队，团队成员具备CNVD（原创漏洞证明）、CCSSP（云计算安全专业能力）、CDPSE（数据隐私安全专家认证）、CISM（信息安全管理认证）、CISSP（信息系统安全专家认证）等证书，提供相关服务人员的社保信息与证书附件材料并加盖原厂公章，以上每满足一项得1分。

三、计算方式及定标办法

采用谈判、询价等价格唯一因素评审的项目，各供应商最终报价相同时的排序办法		最终报价完全相同的，按需求响应情况优劣投票确认排序
采用综合评价法评审的项目，供应商最后得分相同时对供应商进行排序的方法		得分相同的供应商，按竞标报价由低到高顺序排列。得分且报价相同的，按技术指标优劣顺序排列
同品牌投标人获得中标人推荐资格的确定方法		提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格
评定办法	☑综合评价	进行评分，并进行排序（见评分细则）
	☐最低价	符合资格条件和采购需求的最低报价
	☐其他	

（一）本次采购为院内磋商。供应商应派其授权代表持有效身份证件按采购文件规定的时间递交磋商响应文件，并准备参加磋商。

（二）供应商应当在磋商文件“供应商报名须知”要求的截止时间前，将响应文件密封送达磋商会议现场。在截止时间后送达的响应文件为无效文件，磋商小组应当拒收。

（三）供应商在提交响应文件截止时间前，可以对所提交的响应文件进行补充、修改或者撤回。补充、修改的内容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。

（四）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。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。

（五）磋商小组所有成员应当集中与单一供应商分别进行磋商，并给予所有参加的供应商平等的磋商机会。

（六）磋商小组将依据磋商文件要求，对所有供应商提交的磋商文件进行资格评审；对未实质性响应文件要求的，磋商小组应现场告知供应商，取消其参加评标资格。

（七）实质性响应磋商文件资格要求的供应商按所抽取的磋商顺序，依次与磋商小组分别进行磋商。

（八）磋商小组将就磋商文件中的技术、服务要求、合同草案条款等与供应商一一洽谈。

（九）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。

（十）对磋商文件作出实质性变动是磋商或磋商文件的有效组成部分，应当以书面形式同时通知所有参加磋商的供应商。

（十一）磋商结束后，磋商小组将要求不少于三家参加磋商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少于 3 家。最后报价是供应商磋商响应文件的有效组成部分。

（十二）磋商供应商最终报价超过了采购预算，磋商活动终止。

（十三）本次磋商共有三轮报价。三轮报价后，评委对供应商承诺的事项进行综合评议，若出现不能明确推荐第一名或第二名的供应商时，组织与之相对应的供应商进行第四轮报价。

第五章　合同签署

根据《中华人民共和国民法典》，采购人和中标人（成交供应商）之间的权利和义务，应当按照平等、自愿的原则，依据文件要求和响应文件承诺，签订合同。

第六章　响应文件格式

正本/副本

响 应 文 件

项目编码：

项目名称：

供应商名称（全称）：_____（盖章）

供应商法定代表人：_____（签字或盖章）

日期：　年　月　日

响应文件目录（编列要求）

供应商按提供的格式编写目录，目录须标注页码。

编列顺序
1）封面
2）标书目录（含页码）
3）响应函、廉洁承诺书
4）报价汇总表（响应院方采购文件配置需求表）
5）分项报价表（按项目性质编制）
6）法定代表人身份证明书
7）法定代表人授权委托书（授权人参加，格式见附件 1）
8）资格证明文件（按申请人资格要求）
9）需求响应文件
10） 技术响应文件
11） 报价文件
12） 投标企业与被授权人签订的劳动合同和投标企业为被授权人缴纳社保障金的证明材料**（详见第四章评定办法中有关要求）**
13） 财务状况**（详见第四章评定办法中有关要求）**
14） 同类项目业绩的印证材料
15） 供应商认为需要提交的其他文件

格式 1

报价书

襄阳市第一人民医院：

依据贵方（项目名称/采购编号）项目第包采购货物或服务的采购公告，我方代表（姓名、职务）经正式授权并代表供应商（供应商的名称、地址）提交下述文件正本一份，副本四份。

1.响应文件；

2.资格证明文件；

3.有关授权文件。

并进行如下承诺声明：

1．我公司在参加本次采购活动前3年内在经营活动中没有重大违法记录；

2．我公司在本响应文件中所提供的全部资格证明文件均真实有效，我方承诺对其真实性负责并承担相应后果；

3．我公司在本响应文件中所响应的内容均将成为签订合同的依据，并承诺按响应内容提供相应服务；

其它承诺：（如有的话，可自行填写）

在此，我方宣布同意如下：

1.所附《报价一览表》中规定的应提交和交付的货物或服务报价总价为（注明币种，并用文字和数字表示的报价总价）。

2.将按本项目采购文件的约定履行合同责任和义务。

3.已详细审查全部采购文件，包括（补充文件等），对此无异议。

4.本响应文件的有效期自开标之日起共 90 个日历天。

5.接受采购文件中关于诚信履约的约定。

6.同意提供按照贵方可能要求的与其报价有关的一切数据或资料。

供　　应　　商：（公章）

通　讯　地　址：

传　　　　真：　　　　电　　话：

电　子　函　件：

授权 代表 签字：

日　　　　期：

格式 2

法定代表人授权书

兹授权_____同志为我公司参加贵单位组织的（项目名称）采购活动的供应商代表人，全权代表我公司处理在该项目采购活动中的一切事宜。代理期限从年 月日起至年 月日止。

授权单位（签章）：

法定代表人（签字或盖章）：

签发日期：年 月日

附：

代理人工作单位：

职务：性别：

身份证号码：

粘贴被授权人身份证（正反面复印件）：

格式 3

法定代表人身份证明书

兹证明（姓名）在我单位任职务，系（供应商）的法定代表人。

供应商（盖章）：

法定代表人（签章）：

性别：年龄：

身份证号码：

年月日

法定代表人身份证（正反面复印件）：

注：

1、本表适用于供应商不授权代理人,而由法定代表人直接参加磋商并签署响应文件的情况；

2、如供应商具有企业法人代表证书,则还应在本证明书后附上企业法人代表证书复印件。

格式 4

报价一览表

采购项目名称：

采购项目编号：

供应商名称	
供应商地址	
总报价	
工期（供货期）	
质保期	
项目负责人	
投标货物品牌及型号（如有）	
备注	

说明：（1）人民币报价，单位为元，精确到小数点后两位。

（2）此表除保留在竞争性磋商响应文件中外，另复制一份与**报价书、法定代表人身份证明书或法定代表人授权书（原件）、分项报价表（如有要求）**

磋商供应商法定代表人或授权代表签字：

磋商供应商名称（签章）：

时　　间：年月日

格式 5

分项报价表

包号： **报价单位（元 / 万元 ）：**

序号	产品名称	品牌	型号 规格	数量	单价	总价	备注
总价							

注： 1.分项报价总计价格必须与《报价一览表》报价一致。

2.如无分项报价则仅填写拟采购货物报价总价。

投标人名称（加盖单位公章）：_____

法定代表人（或非法人组织负责人）或其授权委托人(签字或盖章)：

日期：_____

格式 6　资格证明文件

格式自拟

格式 7 需求响应文件

格式自拟

格式 8 评审办法响应文件

格式自拟

格式 9

无重大违法记录声明

襄阳市第一人民医院：

我方在此声明，我方在参加本次政府采购活动前三年内，在经营活动中没有以下重大违法记录：

1.我方因违法经营被追究过刑事责任；

2.我方因违法经营被责令停产停业、吊销许可证或者执照；

3.我方因违法经营被处以较大数额罚款等行政处罚。

随本声明附上我方参加本次政府采购活动前 3 年内发生的诉讼及仲裁情况表以及相关的法律证明文件供贵方核验。我方保证上述信息的完整、客观、真实、准确，并愿意承担我方因提供虚假材料谋骗取中标、成交所引起的一切法律后果。

特此声明！

供应商法定代表人或委托代理人签字：

供应商名称（盖章）：

时　间：年月日

格式 10

投标人关联单位及禁止参加情况的承诺函

致：_____

（供应商名称）参加贵院组织的（项目名称）项目(项目编号：_____)的采购活动，本单位郑重声明如下：

本单位未与单位负责人为同一人或者存在直接控股、管理关系的其它供应商，参加本项目同一合同项下的采购活动。

本单位未对本采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务等情形。

我单位对上述声明承诺内容的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（盖章）：_____

法定代表人/单位负责人/自然人/授权代表（签字或印章）:_____

日期：_____年_____月____日