

高县人民医院

信息系统安全三级等保测评

采
购
文
件

高县人民医院
2026 年 10 月

目 录

第一章 比选邀请	1
第二章 比选须知	3
第三章 供应商资格审查及符合性审查	6
第四章 采购需求	9
第五章 评分标准	11
第六章 比选申请文件格式	12

第一章 比选邀请

序号	应知事项	说明和要求
1	采购人	高县人民医院
2	项目名称	信息系统安全三级等保测评项目
3	项目编号	GXRMY-202653
4	采购需求	详见比选文件第四章
5	最高限价	预算 <u>21.6</u> 万元。超过最高限价的报价，其比选申请文件作无效处理。
6	邀请方式	☒ 公开比选：高县人民医院官方网站上以公告形式发布； ☐ 邀请比选：通过书面推荐意见，推荐符合相应资格条件的供应商参与本次采购活动。
7	联合体	☐ 接受 ☒ 不接受
8	现场踏勘	☐ 举行 ☒ 不举行
9	履约保证金	☐ 收取 ☒ 不收取
10	评审方式	☒ 综合评分法 即供应商通过资格审查，且满足比选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， 综合得分最高 的供应商为本项目的第一中选人，若得分相同则价格低的为中选人，若价格也相同则采取 二次议价 的方式确定。 ☐ 最低价评审法 即供应商通过资格审查，且所有技术参数要求和商务要求均符合比选要求，院内评审小组按照有效报价进行详细评审， 有效报价最低 的供应商为本项目的第一中选人，若报价相同则采取 二次议价 的方式确定中选人。

11	比选文件 获取方式	供应商应通过： 高县人民医院官网（网址https://www.scgxrmxy.com/）获取比选文件；本比选文件免费。
12	比选报名时间	2026年10月13日至2026年10月15日，每天8：00 - 12：00，14：30 - 17：30（节假日除外）
13	比选申请人报名时须提供资料	（1）报名表。【格式见附件】 （2）单位介绍信或法人授权书原件，法人及授权代表身份证复印件。 （3）企业法人营业执照副本复印件。 注：上述报名资料均须加盖比选申请人单位公章后，将扫描件发至邮箱：caigouban5393102@163.com。
14	提交比选申请文件方式	现场提交或邮寄： （1）文件份数：正本1份（须盖鲜章）。 （2）邮寄和现场提交地点：宜宾市高县庆符镇硕勋大道西段223号、145号 高县人民医院 行政二楼209采购管理办公室。 注：比选申请文件应在提交比选申请文件截止时间前提交或邮寄送达；未按方式提交或逾期送达或没有密封的比选申请文件恕不接收。
15	提交比选申请文件截止时间	2026年10月 16 日 17 时 30 分
16	比选地点	高县人民医院行政二楼 219（开标室）
17	联系方式	（1）采购部门：采购管理办公室 联系方式：0831-5393102 （2）需求部门：信息科 联系方式：0831-5367378

第二章 比选须知

序号	应知事项	说明和要求
1	报价	(1) 本比选统一使用人民币报价； (2) 报价应是完成比选全部工作内容的价格体现，是最终用户验收合格后的总价，包含了供应商完成本项目所需的一切费用，即项目包干价
2	比选申请文件编制要求	(1) 比选申请文件的格式 比选申请人应仔细阅读本比选文件，按比选文件第六章“比选申请文件格式”进行编制，比选申请人在编制比选申请文件时应使用该章所附格式；该章未规定格式的，由比选申请人根据实际情况自主编制，但不得影响比选申请文件内容的完整性和有效性；比选申请人应在“比选申请文件格式”前附文件索引表、目录； (2) 比选申请文件的签署、盖章 比选申请文件应根据比选文件的要求签署、盖章；
3	评审要求	(1) 原则上供应商应满足三家；若出现不足三家的情形，按本单位采购管理制度相关规定处理。 (2) 院内评审专家应对比选申请人的比选文件进行独立评审。院内评审专家对比选申请人某项指标如有不同意见，按照少数服从多数的原则进行票决，确定该项指标是否通过。符合评审指标通过标准的，为有效响应。 (3) 院内评审小组认为比选申请人的报价明显低于其他通过符合性审查比选申请人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在合理的时间内提供书面说明，必要时提交相关证明材料；比选申请人不能证明其报价合理性的，院内评审小组应当将其作为无效响应处理。 (4) 院内评审小组在评审过程中发现的问题，应当及时作出处理或者向采购办提出处理建议，并作书面记录。 (5) 项目评审当天，比选申请人应保证比选申请文件中所写明的法定代表人或委托代理人的联系方式的畅通，并确保其具备与采购人就本

序号	应知事项	说明和要求
		项目进行沟通。
4	服务质量要求	(1) 符合本比选文件及采购人承诺的质量、技术和其他要求，符合国家相关的质量标准和出厂标准； (2) 国家或行业主管部门对供应商和服务的技术标准和资格资质条件等有强制性规定的，应当符合其要求。
5	知识产权要求	(1) 供应商应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权； (2) 供应商将在比选项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，供应商需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）； (3) 如采用供应商所不拥有的知识产权，则在报价中必须包括合法获取该知识产权的相关费用。
6	供应商纪律要求	(1) 供应商在采购活动中，不得有任何违法乱纪的行为； (2) 若比选申请文件存在虚假响应在评审阶段，院内评审小组应将该比选申请文件作无效处理，若是中选后发现的，采购人应当取消其中选资格； (3) 采购人将对上述行为在其官方网站对相关情况进行通报同时追究其相关法律责任。
7	比选文件澄清、修改	采购人在采购期间发出的一切澄清、修改均为比选文件的有效组成部分
8	供应商质疑	针对采购文件的质疑：自本项目采购公告发布之日起3个工作日内； 针对比选结果的质疑：结果公告发布之日起1个工作日内； 质疑函通过书面形式线下提交。

序号	应知事项	说明和要求
		注： 1.供应商质疑不得超出采购文件、采购过程、采购结果的范围； 2.供应商针对同一采购程序环节的质疑应一次性提出。
9	中选公告	(1) 比选完成后，采购人在医院官网中发出中选公告； (2) 请中选供应商在中选公告发出一个工作日后，联系采购部门老师。 (3) 若中选人以非正当理由放弃中选，在3年内不得参与本单位的比选申请。
10	总体说明	(1) 无论比选结果，供应商的比选申请文件不予撤回，参选产生的一切费用由供应商自行承担； (2) 本比选的第一章、第二章均为实质性要求，供应商应当符合； (3) “采购人”系指本次组织比选的高县人民医院； (4) “供应商”“比选申请人”获取了比选文件拟参加比选和向采购人提供货物及相应服务的供应商； (5) 若采购遇特殊情况，采购人有权终止采购项目； (6) 本比选文件最终解释权归采购人所有。

第三章 供应商资格审查及符合性审查

一、资格要求

序号	资格要求内容	通过条件	备注
1	具有良好的商业信誉和健全的财务会计制度	统一提供承诺函(格式见本文件第四章格式二《承诺函》)	无
2	具有履行合同所必需的设备和专业技术能力		
3	有依法缴纳税收和社会保障资金的良好记录		
4	参加本次采购活动前三年内, 在经营活动中没有重大违法记录		
5	法律、行政法规规定的其他条件		
6	投标企业、生产企业及本次投标涉及产品不得涉及以下情况: 1.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。		
7	供应商应具备独立承担民事责任的能力及行业主管部门要求的各项资质		
8	本项目特定资格要求:	无	

第四章 采购需求

一、项目概括

针对院内 HIS 系统、LIS 系统、PACS 系统、官网、集成平台、互联网医院、慢病系统、远程会诊、双向转诊，共 9 个系统进行等级保护测评。

二、项目服务要求

根据等级保护测评的工作要求，测评范围覆盖安全管理中心、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度。

具体服务内容包括：

（1）协助采购人完成信息系统安全等级保护定级材料编制、专家定级论证材料、备案申报资料整理，全程协助对接属地公安机关网安部门，完成系统备案，直至取得备案回执；因供应商材料编制问题导致备案不通过，由供应商免费修改、补充资料直至备案成功。

（2）差距测评，至少包括：

① 安全技术测评。包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面的安全测评。

② 安全管理测评。包括安全管理制度、安全管理机构、安全管理人员、安全系统建设和安全系统运维五个方面的安全测评。

③ 形成问题汇总及整改意见报告。依据测评结果，对等级测评结果进行汇总统计（测评项符合情况及比例、单元测评结果符合情况比例以及整体测评结果）；通过对信息系统基本安全保护状态的分析给出初步测评结论。根据测评结果制定《系统等级保护测评问题汇总及整改意见报告》，列出被测信息系统中存在的主要问题以及整改意见。

④ 差距测评全部工作须在非诊疗高峰时段实施，所有扫描、测试操作提前向采购人报备，严禁擅自开展破坏性测试；测评过程

中如发现可能影响业务系统运行风险，须立即停止操作并向采购人报告。

(3) 协助完成整改工作。依据整改方案，为安全整改的各项工作提供技术咨询服务。

(4) 等级测评，至少包括：

① 按照等级保护相关标准对系统从安全技术、安全管理等方面进行等级测评工作。

② 编制测评报告，制定并提交《网络安全等级测评报告》，报告需提交公安机关有关部门备案，且能满足合规性要求。新增评测系统提交公安机关进行备案。如果整改，院方按要求整改完毕后，需供应商进行复测（复测费用包含在总报价中，不得另外收取任何费用），并出具复测后的正式报告。

③ 最终出具的《网络安全等级保护测评报告》须符合公安部统一模板，满足四川省、宜宾市公安网安备案审核要求。若因测评报告内容不符合规范被公安退回，供应商必须免费修改、重新出具报告，直至备案通过。

三、三级测评指标

分类	子类	基本要求
安全物理环境	物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内； b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a) 应将设备或主要部件进行固定，并设置明显的不易除去的标识； b) 应将通信线缆铺设在隐蔽安全处。 c) 应设置机房防盗报警系统或设置有专人值守的视频监控系统。
	防雷击	a) 应将各类机柜、设施和设备等通过接地系统安全接地。 b) 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
	防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； b) 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；

		c) 应对机房划分区域进行管理, 区域和区域之间设置隔离防火措施。
	防水和防潮	a) 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透; b) 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透; c) 应安装对水敏感的检测仪表或元件, 对机房进行防水检测和报警。
	防静电	a) 应采用防静电地板或地面并采用必要的接地防静电措施; b) 应采取措施防止静电的产生, 例如采用静电消除器、佩戴防静电手环等。
	温湿度控制	应设置温湿度自动调节设施, 使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a) 应在机房供电线路上配置稳压器和过电压防护设备; b) 应提供短期的备用电力供应, 至少满足设备在断电情况下的正常运行要求; c) 应设置冗余或并行的电力电缆线路为计算机系统供电。
	电磁防护	a) 电源线和通信线缆应隔离铺设, 避免互相干扰; b) 应对关键设备实施电磁屏蔽。
安全通信网络	网络架构	a) 应保证网络设备的业务处理能力满足业务高峰期需要; b) 应保证网络各个部分的带宽满足业务高峰期需要; c) 应划分不同的网络区域, 并按照方便管理和控制的原则为各网络区域分配地址; d) 应避免将重要网络区域部署在边界处, 重要网络区域与其他网络区域之间应采取可靠的技术隔离手段; e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余, 保证系统的可用性。
	通信传输	a) 应采用校验技术或密码技术保证通信过程中数据的完整性; b) 应采用密码技术保证通信过程中数据的保密性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证, 应用程序的关键执行环节进行动态可信验证, 在检测到其可信性受到破坏后进行报警, 并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信; b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制; c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制; d) 应限制无线网络的使用, 保证无线网络通过受控的边界设备接入内部网络。
	访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则, 默认情况下除允许通信外受控接口拒绝所有通信; b) 应删除多余或无效的访问控制规则, 优化访问控制列表, 并保证访问控制规则数量最小化;

		c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
	入侵防范	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
	恶意代码和垃圾邮件防范	a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
	安全审计	a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a) 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
	访问控制	a) 应对登录的用户分配账户和权限； b) 应重命名或删除默认账户，修改默认账户的默认口令； c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在； d) 应授予管理用户所需的最小权限，实现管理用户的权限分离；

	e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； g) 应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
安全审计	a) 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； d) 应对审计进程进行保护，防止未经授权的中断。
入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序； b) 应关闭不需要的系统服务、默认共享和高危端口； c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
数据完整性	a) 应采用校验技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等； b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
数据保密性	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能； b) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地； c) 应提供重要数据处理系统的冗余，保证系统的高可用性。
剩余信息保	a) 应保证鉴别信息所在的存储空间被释放或重新分配前得到完

	护	全清除； b) 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
	个人信息保护	a) 应仅采集和保存业务必需的用户个人信息； b) 应禁止未经授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
	安全管理	a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
	集中管控	a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； c) 应对网络链路、安全设备、网络设备和服务器等运行状况进行集中监测； d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； f) 应能对网络中发生的各类安全事件进行识别、报警和分析。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
	管理制度	a) 应对安全管理活动中的主要管理内容建立安全管理制度； b) 应对管理人员或操作人员执行的日常管理操作建立操作规程； c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
	制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定； b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理	岗位设置	a) 应成立指导和管理网络安全工作的委员会或领导小组，其最

机构		高领导由单位主管领导担任或授权； b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； c) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各工作岗位的职责。
	人员配备	a) 应配备一定数量的系统管理员、审计管理员和安全管理员等； b) 应配备专职安全管理员，不可兼任。
	授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等； b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
	沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和检查	a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； b) 应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
安全管理人员	人员录用	a) 应指定或授权专门的部门或人员负责人员录用； b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
	人员离岗	a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
	安全意识教育和培训	a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； c) 应定期对不同岗位的人员进行技能考核。
	外部人员访问管理	a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

		b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案； c) 外部人员离场后应及时清除其所有的访问权限； d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
安全建设管理	定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； c) 应保证定级结果经过相关部门的批准； d) 应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定； b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
	自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制； b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； c) 应制定代码编写安全规范，要求开发人员参照规范编写代码； d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制； e) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； f) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； g) 应保证开发人员为专职人员、开发人员的开发活动受到控制、监视和审查。
	外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码； b) 应保证开发单位提供软件设计文档和使用指南； c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
	工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理； b) 应制定安全工程实施方案控制工程实施过程； c) 应通过第三方工程监理控制项目的实施过程。

	测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
	系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； b) 应对负责运行维护的技术人员进行相应的技能培训； c) 应提供建设过程文档和运行维护文档。
	等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； b) 应在发生重大变更或级别发生变化时进行等级测评； c) 应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定； b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
安全运维管理	环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； b) 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
	介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a) 应对各种设备(包括备份和冗余设备)、线路等指定专门的部门或人员定期进行维护管理； b) 应对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等； c) 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密； d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
	漏洞和风险	a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞

管理	和隐患及时进行修补或评估可能的影响后进行修补； b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库； h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； b) 应定期验证防范恶意代码攻击的技术措施的有效性。
配置管理	a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和 补丁信息、各个设备或软件组件的配置参数等； b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
密码管理	a) 应遵循密码相关国家标准和行业标准； b) 应使用国家密码管理主管部门认证核准的密码技术和产品。
变更管理	a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施； b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； c) 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
备份与恢复	a) 应识别需要定期备份的重要业务信息、系统数据及软件系统

管理	等; b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等; c) 应根据数据的重要性和数据对系统运行的影响, 制定数据的备份策略和恢复策略、备份程序和恢复程序等。
安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件; b) 应制定安全事件报告和处置管理制度, 明确不同安全事件的报告、处置和响应流程, 规定安全事件的现场处理、事件报告和后期恢复的管理职责等; c) 应在安全事件报告和响应处理过程中, 分析和鉴定事件产生的原因, 收集证据, 记录处理过程, 总结经验教训; d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
应急预案管理	a) 应规定统一的应急预案框架, 包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容; b) 应制定重要事件的应急预案, 包括应急处理流程、系统恢复流程等内容; c) 应定期对系统相关的人员进行应急预案培训, 并进行应急预案的演练; d) 应定期对原有的应急预案重新评估, 修订完善。
外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定; b) 应与选定的外包运维服务商签订相关的协议, 明确约定外包运维的范围、工作内容; c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力, 并将能力要求在签订的协议中明确; d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求, 如可能涉及对敏感信息的访问、处理、存储要求, 对 IT 基础设施中断服务的应急保障要求等。

四、完成项目所需提交的文档清单

在本项目完成后, 供应商须向采购人提交纸质版 (2 套, 加盖公章) + 电子版 (加密 U 盘 1 份) 全部资料, 清单如下:

- 定级备案全套材料 (定级报告、备案表、专家评审材料等)
- 《信息系统安全问题汇总及整改建议》
- 等级保护测评工作过程资料 (现场访谈记录、证据采集记录、测评工作底稿、风险分析记录)
- 《网络安全等级保护等级测评报告》及过程资料
- 复测报告 (如涉及整改复测)

(一) 技术标准和规范

1. 《信息安全等级保护管理办法》
2. 《计算机信息系统安全保护等级划分准则》(GB17859-1999)
3. 《信息安全技术 网络安全等级保护定级指南》
(GB/T22240-2020)
4. 《信息安全技术 网络安全等级保护基本要求》
(GB/T22239-2019)
5. 《信息安全技术 网络安全等级保护测评要求》
(GB/T28448-2019)
6. 《信息安全技术 网络安全等级保护测评过程指南》
(GB/T28449-2018)

(二) 安全要求

成交供应商在项目实施过程中，必须遵守以下技术原则：

1 保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购方的行为，否则采购方有权追究供应商的责任。

2 标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

3 规范性原则：供应商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制，测评出具的报告须符合公安部颁布的《信息系统安全等级测评报告模板》。

4 可控性原则：等保测评服务的进度要按照招标文件 的要求，保证采购方对于测评工作的可控性。

5 整体性原则：等保测评服务的范围和内容应当整体全面，包括国家等级保护相关要求测评要求涉及各个层面。

6 安全性原则：等保测评服务工作应不得影响系统和网络的正常运行；测评工作不得对现有信息系统的正常运行、业务的正常开展产生任何影响。

7. 测评机构资质及人员要求：

(1) 从事信息系统检测评估相关工作人员无违法记录。

(2) 工作人员仅限于中华人民共和国境内的中国公民,且无犯罪记录。

(3) 测评期间需遵守被测单位相关管理规定,禁止利用测评工作从事危害被测单位利益、安全的活动。

(4) 项目总测评师须具有网络安全等级测评师高级证书

五、商务要求

(一) **服务期限:** 合同签订后 60 日内完成。

(二) **付款方式:** 合同签订后,测评完成并出具最终测评报告,并通过院方验收后,收到供应商增值税发票,15 个工作日后,支付金额为合同总金额 100%。

(三) 项目验收方案

由采购人成立验收小组,组织验收工作,按照本采购需求及合同约定开展履约验收,供应商配合提供全部佐证材料。

验收合格须同时满足下列全部条件: ①全套文档资料完整交付,提供加盖供应商公章纸质资料 2 套及加密电子版,包含定级备案材料、差距测评整改建议材料、正式测评报告、复测报告(如有)、安全管理制度模板; ②出具符合规范的正式等级保护测评报告,满足属地公安网安部门备案要求,完成备案并取得备案回执;因供应商报告编制问题导致备案材料被退回的,由供应商免费修改直至备案通过; ③差距测评、整改咨询、复测服务(如有)全部履约完成; ④项目实施期间未发生业务中断、患者敏感信息泄露等安全事故。

验收流程: 供应商完成全部服务后提交验收申请及全套交付成果,采购人收到申请后 10 个工作日内组织验收。验收不合格的,供应商须在采购人指定期限内无偿完成整改并重新申请验收。

(四) 履约保证金缴纳及退还要求

无

(五) 付款方式

合同签订后,测评完成并出具最终测评报告,并通过院方验收

后，收到供应商增值税发票，15 个工作日后，支付金额为合同总金额 100%。

（六）项目售后服务要求

项目自验收合格之日起须提供 12 个月技术支撑期：

1. 如遇上级监管部门检查等要求时，供应商提供远程技术支持；需要现场支撑的，接到采购人通知后，48 小时内安排工程师上门，不收取额外任何费用；

2. 提供等保相关政策咨询、报告答疑；

（七）双方违约责任

1. 甲方违约责任

（1）甲方未按合同约定支付款项的，每逾期一日，按应付未付金额的万分之五向乙方支付违约金；逾期超过【30】日，乙方有权暂停履行合同义务；逾期超过【60】日，乙方有权解除合同，甲方除支付应付款项外，还应当赔偿乙方全部实际损失。

（2）因甲方原因造成乙方无法正常履行合同的，甲方应当承担由此产生的全部损失；造成工期 / 交付延期的，交付期限相应顺延。

2. 乙方违约责任

（1）乙方未按约定时间完成交付 / 提供服务的，每逾期一日，按合同总价款的万分之五向甲方支付违约金；逾期达到【30】日，甲方有权解除合同，乙方应当退还甲方已支付款项，并赔偿甲方损失。

（2）乙方交付成果 / 提供服务不符合合同质量标准的，乙方应在【30】日内无偿整改、重做；经两次整改仍达不到约定标准的，甲方有权解除合同，乙方退还全部已付款项，并承担相应赔偿责任。

六、评审规则

序号	评分项目	分值	评分标准
1	报价	20	经评审有效报价的最低价作为评标基准价，投标报价得分=(评标基准价 / 投标报价)×20。
2	业绩	10	具有类似三级等保测评项目案例（2023 年 1 月 1 日至投标文

			件递交截止日），每有一个得 2 分，最多得 10 分；提供合同复印件加盖单位鲜章。	
4	投入本项目的专业技术力量	30	总测评师 (9)	总测评师具有公安部信息安全等级保护评估中心或中关村信息安全测评联盟或公安部关键信息基础设施保护中心颁发的信息（或网络）安全等级测评师（高级）证书、人社部门评定颁发的中级及以上工程师职称证书（专业：数据安全或网络安全服务；因各地职称专业命名存在地域差异，证书专业名称与前述名称实质一致的也予以认可）、中国信息安全测评中心颁发的注册信息安全专业人员(CISP)证书的每有一项得 3 分，最多得 9 分。 注：须提供证书复印件；在职证明可提供加盖单位鲜章的在职证明，或近 3 个月社保缴纳凭证，二者任选其一，加盖单位鲜章。
5			技术团队 (21)	1、项目技术负责人具有公安部信息安全等级保护评估中心或中关村信息安全测评联盟或公安部关键信息基础设施保护中心颁发的信息（或网络）安全等级测评师（中级及以上）证书、人社部门评定颁发的中级及以上工程师职称证书（专业：数据安全或网络安全服务；因各地职称专业命名存在地域差异，证书专业名称与前述名称实质一致的也予以认可）、人力资源和社会保障部和工业和信息化部颁发的信息系统项目管理师证书的每有一项得 3 分, 最多得 9 分。 2、项目质量负责人具有公安部信息安全等级保护评估中心或中关村信息安全测评联盟或公安部关键信息基础设施保护中心颁发的信息（或网络）安全等级测评师证书，得 3 分。 项目质量负责人具有人力资源和社会保障部和工业和信息化部颁发的系统规划与管理师证书、软件评测师

			证书的每有一项得 1 分,最多得 2 分。 3、测评团队专业技术人员(除总测评师、技术负责人、质量负责人以外)具有人社部门评定颁发的中级及以上工程师职称证书(专业方向包含数据安全或网络安全服务;因各地职称专业命名存在地域差异,证书专业名称与前述名称实质一致的也予以认可。)、公安部信息安全等级保护评估中心或中关村信息安全测评联盟或公安部关键信息基础设施保护中心颁发的信息(或网络)安全等级测评师(中级及以上)证书,每有一项得 3 分,最多得 6 分。 4、测评团队专业技术人员(除总测评师、技术负责人、质量负责人以外)具有人力资源和社会保障部和工业和信息化部颁发的系统分析师证书,得 1 分。 注:须提供证书复印件;在职证明可提供加盖单位鲜章的在职证明,或近 3 个月社保缴纳凭证,二者任选其一,加盖单位鲜章。
6	测评方案	40	根据本项目制定完整的等保测评方案包括(①安全物理环境②安全通信网络③安全区域边界④安全计算环境⑤安全管理中心⑥安全管理制度⑦安全管理机构⑧安全管理人员⑨安全运维管理⑩安全建设管理)的得 40 分,每缺一项方案扣 4 分;提供的方案中每有一处具有缺陷(缺陷是指:存在不适用项目实际情况的情形、凭空编造、方案中内容前后不一致、前后逻辑错误、涉及的规范及标准错误、不符合项目实际情况等)的扣 2 分,扣完为止。

第五章 评分办法

供应商通过资格审查，且满足比选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，**综合得分最高**的供应商为本项目的第一中选人，若得分相同则价格低的为中选人，若价格也相同则采取抽签的方式确定。

第六章 比选申请文件格式

（比选申请封面）

项目名称：

项目编号：

比选申请文件

比选申请人名称（公章）：

法定代表人或授权代理人（签字）：

联系方式（移动电话）：

日期： 年 月 日

一、承诺函

致高县人民医院：

本公司_____（公司名称）参加_____（项目名称）的比选活动，现承诺：

我公司满足关于比选申请人的资格要求，包括（不限于）：

- （1）具有独立承担民事责任的能力；
- （2）具有良好的商业信誉；
- （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；
- （7）根据采购项目提出的特殊条件。
- （8）截止比选时间未被列入“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)渠道信用记录失信被执行人、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；未处于政府部门禁止代理政府采购业务处罚期、未在我院禁止参与期内。

2. 我方已认真阅读并接受本项目比选文件的全部实质性要求，如对比选文件有异议，已依法进行维权救济，不存在对比选文件有异议的同时又参加比选以求侥幸成交或者为实现其他非法目的的行为。

3. 本项目比选有效期为 90 天。

4. 比选申请文件中提供的任何资料和技术、服务、商务等响应承诺情况都是真实的、有效的、合法的。

5. 如本项目比选采购过程中需要提供样品，则我方提供的样品即为成交后将要提供的成交产品，我方对提供样品的性能和质量负责，因样品存在缺陷或者不符合比选文件要求导致未能成交的，我方愿意承担相应不利后果。

6. 国家或行业主管部门对采购产品的技术标准、质量标准和资格资质条件等有强制

性规定的，我方承诺符合其要求。

7. 参加本次采购活动，我方完全同意比选文件“合同分包”、“合同转包”的实质性要求，并承诺严格按照比选文件要求履行。

8. 我方保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由我方承担所有相关责任。除非比选文件特别规定，采购人享有本项目实施过程中产生的知识成果及知识产权。如我方在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，我方承诺提供开发接口和开发手册等技术资料，并提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。如我方在项目实施过程中采用非自有的知识产权，则在报价中已包括合法获取该知识产权的相关费用。

9. 我方自愿按照比选文件规定的各项要求向采购人提供所需货物和服务。

10. 一旦我方成交，我方将严格履行采购合同规定的责任和义务。

11. 我方愿意提供贵单位可能另外要求的，与比选报价有关的文件资料，并保证我方已提供和将要提供的文件资料是真实、准确的。

12. 我方承诺向贵单位供货的同规格型号同质量等级医用物资低于市场价，办公用品、装修材料、工会福利等为同时期宜宾市内采购最低价。

本单位对上述承诺的内容事项真实性负责。如经查实上述承诺的内容事项存在虚假，我单位愿意接受以提供虚假材料谋取成交追究法律责任。

比选申请人名称： （盖章）

时间：

承诺函

致：高县人民医院

针对本项目建设需求，我司郑重承诺，本项目所开发、对接的全部接口，均完全适配采购单位现有体检系统：天方达杏林七贤体检中心管理系统软件（版本号：V18.7），可实现系统无缝对接、数据正常互通、业务流程顺畅联动，完全满足本项目对接及使用要求。

我司保证所提供的接口适配服务合规、稳定、兼容，如因接口不匹配、无法适配现有系统导致项目无法验收或无法正常使用，我司将无条件免费整改、优化直至完全达标，并承担由此产生的全部责任及相关损失。

本承诺函真实有效，具有法律效力。

特此承诺！

承诺单位（盖章）：_____

法定代表人/授权代表人（签字）：_____

日 期：_____年____月____日

二、具有独立承担民事责任的能力

(营业执照)

三、具有健全的财务会计制度的证明材料

四、法定代表人身份证明书

(若为法定代表人/单位负责人参与则提供此页)

_____(姓名)系_____ (比选申请人名称)的法定代表人/单位负责人(职务:_____,电话:_____)。
特此证明。

比选申请人名称: (盖章)

时间:

注:

1. 比选申请人为自然人时提供“自然人身份证明材料”。
2. 应附法定代表人/单位负责人身份证明材料复印件(提供其在有效期的材料,如居民身份证正、反面复印件)。
3. 身份证明材料包括居民身份证或户口本或军官证或护照等。
4. 此授权书盖章位置未做强制性要求。

(若委托授权代表参与则提供此页)

委托代理人无转委托权。特此委托。

委托代理人： (签字)

时间:

1. 应附法定代表人/单位负责人和委托代理人的身份证明材料复印件（提供其在有效期内的材料，如居民身份证正、反面复印件）。
2. 身份证明材料包括居民身份证或户口本或军官证或护照等。
3. 此授权书盖章位置未做强制性要求。

七、开标一览表

项目名称：信息系统安全三级等保测评项目

系统名称	投标单价（元）	备注
HIS 系统		
LIS 系统		
PACS 系统		
官网		
集成平台		
互联网医院		
慢病系统		
远程会诊		
双向转诊		
投标总价	大写： 小写：	

注：1. 投标人投标总价超过本项目最高限价的，做无效投标处理。

2. 供应商的报价应该包括等保测评费、人工费、税费、备案等以及与本项目相关的一切其他费用。

3. “开标一览表”须填报各子系统对应费用的单价，同时列明项目总报价。

投标人名称：XXXX（单位公章）

法定代表人/单位负责人或授权代表（签字或加盖个人名章）：XXXX

投标日期：XXXX

八、第四章采购需求承诺函

九、供应商认为需要提供的其他材料

• • • • • （格式自拟）