第三章 磋商项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

3.1、采购项目概况

为贯彻落实《中华人民共和国网络安全法》、《信息安全等级保护管理办法》、《公安部关于贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》等国家相关法律法规，不断提高网络安全整体防护能力，成都市第五人民医院启动了年度信息系统网络安全等级保护测评工作。成都市第五人民医院拟采购信息安全等级保护测评服务项目一项，本项目为1个包。

3.2、服务内容及服务要求

3.2.1服务内容

采购包1：

采购包预算金额（元）: 360,000.00

采购包最高限价（元）: 360,000.00

序号	标的名称	数量	标的金额 （元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	2024年信息安全等级保护测评服务	1.00	360,000.00	项	软件和信息技术服务业	否	否	否	否

3.2.2服务要求

采购包1：

标的名称：2024年信息安全等级保护测评服务

参数性质	序号	技术参数与性能指标
		（一）测评内容

序号	系统名称	安全保护等级
1	HIS	第三级
2	LIS	第三级
3	PACS	第三级
4	EMR	第三级
5	门户网站	第三级
6	HRP	第三级
7	医院信息平台	第三级
8	OA系统	第三级
9	互联网医院	第三级

（二）工作内容

1、等级测评的现场实施过程由单元测评和整体测评两部分构成。对应《基本要求》各安全控制点的测评称为单元测评，具体可分为：（1）安全物理环境、（2）安全区域边界、（3）安全通信网络、（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）安全建设管理、（10）安全运维管理等10个测评任务。整体测评是在单元测评的基础上，通过进一步分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评，具体如下：

（1）安全物理环境测评实施具体测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	物理位置选择	通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。
3	防盗窃和防破坏	通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。
5	防火	通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。
6	防水和防潮	通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。
7	防静电	通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。
9	电力供应	通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。
10	电磁防护	通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。

（2）安全通信网络测评实施具体测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	网络架构	测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	通信传输	测评通信过程中的完整性、保密性等。
3	可信验证	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，并在应用程序的关键执行环节进行动态可信验证。

（3）安全区域边界测评实施具体的测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	边界防护	测评分析信息系统网络边界安全防护的状况。
2	访问控制	测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力
3	入侵防范	测评分析信息系统对攻击行为的识别和处理情况。
4	恶意代码和垃圾邮件防范	测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮的防护情况。
5	安全审计	测评分析信息系统审计配置和审计记录保护情况。
6	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数通信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信验证。

（4）安全计算环境测评实施具体的测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	身份鉴别	检查服务器的身份标识与鉴别和用户登录的配置情况。
2	访问控制	检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。
3	安全审计	检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。
4	入侵防范	检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。
5	恶意代码防范	检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。
6	可信验证	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，并在应用程序的关键执行环节进行动态可信验证。
7	数据完整性	测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。
8	数据保密性	测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。
9	数据备份恢复	测评信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。
10	剩余信息保护	测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。
11	个人信息保护	测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。

（5）安全管理中心测评实施具体的测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	系统管理	测评信息系统的系统管理员对系统的管理情况。
2	审计管理	测评信息系统的安全审计员对系统的审计情况。
3	安全管理	测评信息系统的安全管理员对系统的安全策略的配置情况。
4	集中管控	测评网络链路、安全设备、网络设备和服务器等设备的运行状况集中监测、分析、报警等。

（6）安全管理制度测评实施具体测评指标描述如下表所示。

★ 1

序号	安全子类	测评指标描述
1	安全策略	测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。
2	管理制度	测评信息系统管理制度在内容覆盖上是否全面、完善。
4	制定和发布	测评信息系统管理制度的制定和发布过程是否遵循一定的流程。
5	评审和修订	测评信息系统管理制度定期评审和修订情况。

（7）安全管理机构测评实施具体测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	岗位设置	测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。
2	人员配备	测评信息系统各个岗位人员配备情况。
3	授权和审批	测评信息系统对关键活动的授权和审批情况。
4	沟通与合作	测评信息系统内部部门间、与外部单位间的沟通与合作情况。
5	审核和检查	检查信息系统安全工作的审核和测评情况。

（8）安全管理人员测评实施具体测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	人员录用	测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。
2	人员离岗	测评信息系统人员离岗时是否按照一定的手续办理。
3	安全意识教育和培训	测评是否对人员进行安全方面的教育和培训。

4	外部人员访问管理	测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

（9）安全建设管理测评实施具体测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	定级和备案	测评是否按照一定要求确定系统的安全等级并完成备案工作。
2	安全方案设计	测评系统整体的安全规划设计是否按照一定流程进行。
3	产品采购和使用	测评是否按照一定的要求进行系统的产品采购。
4	自行软件开发	测评自行开发的软件是否采取必要的措施保证开发过程的安全性。
5	外包软件开发	测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。
6	工程实施	测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。
7	测试验收	测评系统运行前是否对其进行测试验收工作。
8	系统交付	测评是否采取必要的措施对系统交付过程进行有效控制。
9	等级测评	测评是否依据国家要求完成等级测评和整改工作。
10	服务供应商选择	测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

（10）安全运维管理测评实施具体测评指标描述如下表所示。

序号	安全子类	测评指标描述
1	环境管理	测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。
2	资产管理	测评是否采取必要的措施对系统的资产进行分类标识管理。
3	介质管理	测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。
4	设备维护管理	测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。

5	漏洞和风险管理	测评是否采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补。测评是否定期开展安全测评。
6	网络和系统安全管理	测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。
7	恶意代码防范管理	测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。
8	配置管理	测评是否记录和保存系统的基本配置信息
9	密码管理	测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。
10	变更管理	测评是否采取必要的措施对系统发生的变更进行有效管理。
11	备份与恢复管理	测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。
12	安全事件处置	测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。
13	应急预案管理	测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。
14	外包运维管理	测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。

安全控制点间安全测评：

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。

区域间/层面间安全测评：

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。

3.2.3人员配置要求

采购包1：

供应商需为本项目配置项目经理、技术负责人、项目团队成员。（此项对应综合评分明细表中人员配置评分）

3.2.4设施设备要求

采购包1：

详见3.2.2服务要求。

3.2.5其他要求

采购包1：

★1.供应商须提供有效期内的《网络安全等级测评与检测评估机构服务认证证书》。（提供有效证书复印件） ★2.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，必须符合其要求。（实质性要求，供应商须在服务要求应答表进行响应。） 3.供应商需为本项目制定技术方案，包含①项目实施流程②项目管理③测评风险控制④项目实施时间计划⑤项目组织架构。 4.提供供应商自2021年1月1日（含）以来（至递交响应文件截止时间）具有类似信息安全测评项目业绩。（3.4项对应综合评分明细表中的评分）

3.3、商务要求

3.3.1服务期限

采购包1：

自合同签订之日起90日

3.3.2服务地点

采购包1：

★ 成都市第五人民医院。（注：3.3.2服务地点为实质性要求，供应商须在商务应答表进行响应。）

3.3.3考核（验收）标准和方法

采购包1：

★ 1.技术履约内容及标准： 按国家有关规定以及本项目采购文件的技术要求、供应商的响应文件及承诺与本合同约定标准进行技术履约验收。 ★ 2.商务履约内容及标准： 按照采购文件商务要求及供应商响应内容进行商务履约验收。 ★ 3.验收要求 GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》 GB/T 25058-2019：《信息安全技术 网络安全等级保护实施指南》 GB/T 28448-2019：《信息安全技术 网络安全等级保护测评要求》 GB/T 28449-2018：《信息安全技术 网络安全等级保护测评过程指南》 验收时，成交供应商需出具《等级测评报告》，每个系统一式两份并协助采购人向成都市公安局对各系统的信息安全等级保护测评成功备案。 ★4.质量要求：按国家相关规定执行。 ★ 5.其他未尽事宜将按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》(财库(2016) 205号)、《政府采购需求管理办法》(财库(2021) 22号)的要求及国家行业主管部门规定的标准、方法和内容进行验收。（注：3.3.3考核（验收）标准和方法均为实质性要求，供应商须在商务应答表进行响应。）

3.3.4支付方式

采购包1：

一次付清

3.3.5支付约定

采购包1： 付款条件说明： 乙方协助甲方完成2024年信息安全等级保护测评项目并经验收合格，同时在成都市公安局全部成功备案后，待乙方提供正式发票及凭证资料 ，达到付款条件起 14 日内，支付合同总金额的 100.00%。

3.3.6违约责任及解决争议的方法

采购包1：

★1、甲乙双方必须遵守并执行项目中的各项规定，保证本项目的正常履行。 ★2、甲方无故逾期付款的，除应及时付足款项外，应向乙方偿付欠款总额万分之五/天的违约金；逾期付款超过30天的，乙方有权终止合同。 ★3、乙方延迟交付超过7日的，除应及时完成交付内容外，应向甲方偿付合同总额万分之五/天的违约金；延迟交付超过30天的，甲方有权终止合同。如果甲方选择解除合同，乙方除支付上述违约金外，应当全额退还甲方已经付的合同款项，并对给甲方造成的损失承担赔偿责任。 ★4、如因乙方工作人员在履行职务过程中的疏忽、失职、过错等故意或者过失原因给甲方造成损失或侵害，包括但不限于甲方本身的财产损失、由此而导致的甲方对任何第三方的法律责任等，乙方应支付合同总价15%的违约金，并承担全部的赔偿责任。 ★5、变更、中止或者终止合同，有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。（注：3.3.6违约责任及解决争议的方法均为实质性要求，供应商须在商务应答表进行响应。）

3.4其他要求

★（1）服务期限：在2024年8月15日以前完成本条第（一）款项下的9项测评内容。（因系统固化原因，3.3.1服务期限不适用于本项目，以本条为准） ★（2）付款方式：成交供应商协助采购人完成2024年信息安全等级保护测评项目并经验收合格，

同时在成都市公安局全部成功备案后，待供应商提供正式发票的10个工作日内一次性支付全额价款。注：付款前，供应商须向采购人出具合法有效完整的完税发票及凭证资料，否则采购人可以拒付当笔款项并不视为违约，供应商应继续履行约定义务。（因系统固化原因，3.3.4及3.3.5支付约定不适用于本项目，以本条为准）（注：3.4其他要求★（1）服务期限及★（2）付款方式均为实质性要求，供应商须在商务应答表进行响应。） 其他说明（本说明无需供应商进行响应）： 1、根据《财政部关于公布废止和失效的财政规章和规范性文件目录（第十四批）的决定》,《财政部 国家发展改革委信息产业部关于印发无线局域网产品政府采购实施意见的通知》（财库〔2005〕366号）已废止。因系统固化原因，采购文件第二章《供应商须知前附表》序号5“落实节能、环保、无线局域网”中第4条不适用于本项目。 2、针对磋商文件第二章2.4.9中“供应商应按照客户端操作要求，对应磋商文件的每项实质性要求，逐一如实响应”，除磋商文件中的明确要求进行单独响应或承诺的实质性要求外，对于其他实质性要求，供应商在《投标（响应）函》中以“我单位完全接受和理解本项目采购文件规定的实质性要求”进行承诺即视为逐一如实响应。