东莞市松山湖中心医院

2026年网络安全等级保护测评服务采购参数

一、项目背景

为贯彻落实国家、公安机关的等级保护测评工作的相关要求，进一步提升医院的信息化水平和运行效率，加强重要信息系统网络安全等方面的管理，规范信息系统安全机制建设，提高重要信息系统运行环境安全。因此，需要委托具有国家承认测评资质的测评机构对本单位核心信息系统展开第三方测评服务，提供7个信息系统的等级保护测评服务工作，为信息系统提供安全保障。

二、 预算金额：16万元

三、 支付方式：

合同签订后采购方凭中标人开具的等额正规发票15个工作日内支付合同总额的30%，完成验收测评及测评备案后，采购方凭中标方提交的加盖等保测评章的《网络安全等级保护测评报告》、等额正规发票及验收报告后15个工作日内支付支付合同总额的70% 。

四、 采购内容

（一）采购内容

供应商须严格遵照国家现行最新网络安全等级保护标准及配套测试规范，根据采购人相关要求，承接并完成采购人7个核心信息系统的三级网络安全等级保护测评全部服务工作，确保测评流程、检测依据、合规判定均符合最新官方标准要求。

（二）服务内容

服务时限说明：自中选通知书发出之日起15个工作日内签订合同，自合同签订生效之日起80个工作日内出具成果文件。

1、技术服务依据

信息系统安全服务主要依据如下技术标准（下述标准若有更新，以最新标准为准）

1、《中华人民共和国网络安全法》

2、《网络安全等级保护管理办法》

3、《信息安全技术 网络安全等级保护定级指南》（GBT22240-2020）

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安全设计技术要求》（GBT25070-2019）

7、《信息安全技术 信息系统安全等级保护测评过程指南》（GB/T 28449-2018）

2、差距测评

网络安全等级保护差距测评应包括两方面的内容：

2.1、安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况。

安全控制测评使用测评单元方式组织，分为安全技术测评和安全管理测评两大类。

（1）安全技术测评

①安全物理环境。通过访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况。主要涉及对象为机房及相关配套设施。

②安全通信网络。通过访谈、配置检查和工具测试的方式测评信息系统的网络安全保障情况。主要涉及对象为网络互联设备、网络安全设备和网络拓扑结构等三大类对象。

③安全区域边界。将通过访谈、配置检查和工具测试的方式测评信息系统的网络边界安全保障情况。重点测评的包括各边界防火墙，交换机等。

④安全计算环境。通过访谈、配置检查和工具测试的方式测评信息系统的操作系统、数据库等保障情况。

⑤安全管理中心。通过访谈、配置检查的方式测评信息系统的安全管理中心保障情况，主要涉及对象为纳入测评范围的安全管理中心等。

（2）安全管理测评

①安全管理制度。通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。

②安全管理机构。通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

③安全管理人员。通过访谈和检查的形式评测机构人员安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

④安全建设管理。通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记

录等对象。

⑤安全系统运维。通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。

2.2、系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关。在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，分析评估安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性。

2.3、综合测评总结将在安全控制测评和系统整体测评两个方面的内容基础上进行，由此而获得信息系统对应安全等级保护级别的符合性结论。

网络安全等级保护测评方法至少应包括人员访谈、文档检查和系统测试等。

（1）人员访谈：通过与信息系统有关人员进行交流、讨论等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。

（2）文档检查：通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全保护措施是否有效的一种方法。

（3）系统测试：依照相关标准与法律法规实施测评，使用等级保护检查工具作为主要的系统检查、信息收集、分析工具，同时结合其他专业脆弱性安全扫描工具、安全配置核查工具的扫描分析结果作为参考。将该阶段搜集的数据信息录入系统测评核查表，以供后期分析。配置核查扫描提供每个扫描任务的日志文件报告，方便后期进行行为审计。

依照《信息系统安全等级保护基本要求》进行逐个对照，由具备等级测评师、 网络与信息安全管理员或同等技术能力资质的服务人员对信息系统安全情况与等级保护基本要求的差距进行评估，完成信息系统等级保护差距分析报告。

3、协助安全建设整改

依据信息系统测评结果，针对不符合项、系统漏洞和系统风险点，提出安全整改建议。主要从层面内安全、层面间安全、区域间安全、系统结构安全进行整体评估，总结关键

风险点，并形成安全整改方案。协助指导采购人完成信息系统信息安全整改，达到国家规定的网络安全等级保护相关要求。

4、等级保护验收测评

根据安全整改建设情况，对信息系统进行验收测评，按照公安部制定的网络安全等级测评报告格式编制等级测评报告，并协助采购人向公安机关提交符合要求的等级保护验收测评报告，完成测评备案及验收工作。

5、等级保护测评工具要求

测评服务机构应提供正版的国产漏洞扫描、安全检测管理工具，并使用在省级网络安全等级保护协调小组办公室备案的网络安全等级保护测评软件系统开展服务。所提供的网络安全等级保护测评系统具有融合自动化工具和第三方安全检查工具检查、扫描的功能，包含系统调研模块、方案编制模块、现场测评模块、评分与风险分析模块、报告编制模块和工具测试模块。

五、 资质要求

中标方须具有公安部第三研究所颁发“网络安全等级测评与检测评估机构服务认证证书”。

六、 项目完工期要求

（1）合同签订后 30 天内，中标人需完成上述 7 个核心信息系统三级等级保护初次测评工作，并提交相关初次测评结果或问题汇总及安全整改建议；

（2）医院在完成安全建设整改后，30 天内中标人完成上述 7 个核心信息系统三级等级保护验收测评工作，并提交符合国家标准的《网络安全等级保护【被测评对象】等级测评报告》。

七、 人员要求

在项目实际执行过程中，须在合同签定后组建能胜任相关工作的项目组开展工作，如项目经理或项目组成员不能胜任相关工作的，采购人有权要求更换，否则采购人有权终止合同并报相关管理部门进行处理。

项目实施的主要人员未经用户同意不得调整；测评服务机构如中途更换项目经理和主要技术人员，应征得用户同意，否则采购人有权终止合同。

中标人为本项目成立等级保护测评服务项目组，参与本项目的人员不少于 6 人（项目经理 1 人和成员不少于 5 人）。项目经理具有一定的管理能力和等保测评相关的项目经验，接受医院的统一管理。中标人为本项目成立的项目组的人员须固定，如有变更，须经医院书面同意。

八、 验收标准

7 个核心信息系统通过三级等保测评，并提交包括但不限于下列交付物：

工作阶段	服务交付物
差距评估阶段	《等级保护测评问题单及整改建议》
等级测评阶段	《信息系统网络安全等级测评报告》

九、 保密要求

测评服务机构应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人保密信息应严格保守，保证不被披露或使用，包括意外或过失。

测评服务机构不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人保密信息；不得直接或间接地向无关人员泄露采购人的保密信息；不得向不承担保密义务的任何第三人披露采购人的保密信息。测评服务机构在从事服务工作时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及本项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或机构内部与该项目无关的任何人员。

测评服务机构对于工作期间知悉采购人的保密信息（包括业务信息在内）或工作过程中接触到的单位文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。测评服务机构严禁泄露在工作中接触到的科技研究、发明、装备器材及其技术资料和工作信息。