2025年度等级保护测评服务项目采购需求

一、项目基本情况

（一）项目名称：2025年度等级保护测评服务项目

（二）预算金额：120万元，超此预算价为无效报价

（三）本项目（是/否）接受联合体投标：否

二、申请人的资格要求

（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政府采购活动。

（三）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。

（四）未被列入失信被执行人、重大税收违法失信主体，未被列入政府采购严重违法失信行为记录名单。

（五）落实政府采购政策需满足的资格要求：无。

（六）本项目的特定资格要求：

1. 投标人必须具有公安部第三研究所颁发的有效期内的《网络安全服务认证证书等级保护测评服务认证》（需提供证书复印件并加盖公章）。

2. 投标人2024年1月1日至今（以合同签订时间为准）至少具有3项（含三级系统）安全等级保护测评业绩。（提供合同复印件或中标通知书并加盖公章）。

三、采购需求

（一）项目背景

为了落实网信办、公安部和上级主管部门关于网络安全等级保护要求，进一步增强系统安全防护能力，保障系统安全稳定运行。现依据《中华人民共和国网络安全法》和《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》等法律法规和标准规范开展网络安全等级保护工作。

投标人需根据测评中发现的安全问题，协助采购人开展安全整改工作，健全网络安全保护设施，完善安全管理制度，落实安全责任，确保安全整改结果满足等级保护标准要求，提供等级保护配置核查、建设咨询等安全服务。

（二）项目系统范围

武汉市卫生健康信息中心负责的31重要信息系统。

（三）标准规范

- 《中华人民共和国网络安全法》
- 《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)
- 《国家信息化领导小组关于加强信息安全保障工作的意见》 (中办发[2003]27 号)
- 《关于信息安全等级保护工作的实施意见》(公通字 [2004]66 号)
- 《信息安全等级保护管理办法》(公通字 [2007]66 号)
- 《关于开展全国重要信息系统安全等级保护定级工作的通 知》(公信安[2007]861 号)
- 《信息安全等级保护备案实施细则》(公信安 [2007]1360 号)
- 《公安机关信息安全等级保护检查工作规范》(公信安 [2008]736 号)

- 《关于开展信息安全等级保护安全建设整改工作的指导意 见》(公信安[2009]1429 号)
- 《关于推动信息安全等级保护测评体系建设和开展等级测 评工作的通知》(公信安 [2010]303 号)
- 《关于印发医疗卫生机构网络安全管理办法的通知》（国卫规划发〔2022〕29 号）
- 《关于印发紧密型县域医共体信息化功能指引的通知》（国卫办规划函〔2025〕63 号）
- 《GB/T22239-2019 信息安全技术 网络安全等级保护基本要求》
- 《GB/T25070-2019 信息安全技术 网络安全等级保护设计技术要求》
- 《GB/T28448-2019 信息安全技术 网络安全等级保护测评要求》
- 《GB/T28449-2018 信息安全技术 网络安全等级保护测评过程指南》
- 《GB/T25058-2019 信息安全技术 信息系统安全等级保护实施指南》
- 《GB/T22240-2020 信息安全技术 网络安全等级保护定级指南》

（四）定级备案服务

按照《GB/T22240-2020 信息安全技术 网络安全等级保护定级指南》等要求完成新增系统的定级备案工作，取得武汉市公安局颁发的备案证明。

（五）等级测评服务

1. 服务目标

按照《GB/T22239-2019 信息安全技术 网络安全等级保护基本要求》等标准开展差距测评和二次测评工作，出具符合要求的安全等级保护测评报告。

2. 测评内容

依据等级保护政策要求、技术标准和管理规范以及行业要求开展测评，内容包括但不限于以下内容：

（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、安全计算环境和安全管理中心等五个方面的安全测评；

（2）安全管理测评：包括安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评；

（3）系统整体测评：包括安全控制点测评、安全控制点间测评和区域间测评。

- 安全物理环境

针对物理机房提出的安全控制要求。主要对象为物理环境、物理设备和物理设施等；涉及的安全控制点包括物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护。

- 安全通信网络

针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网等；涉及的安全控制点包括网络架构、通信传输和可信验证。

- 安全区域边界

针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等；涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证。

- 安全计算环境

针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象，包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等；涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护。

- 安全管理中心

针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

- 安全管理制度

针对整个管理制度体系提出的安全控制要求，涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订。

- 安全管理机构

针对整个管理组织架构提出的安全控制要求，涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查。

- 安全管理人员

针对人员管理提出的安全控制要求，涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理。

- 安全建设管理

针对安全建设过程提出的安全控制要求，涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评和服务供应商管理。

- 安全运维管理

针对安全运维过程提出的安全控制要求,涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理。

- 安全控制点测评是对单个控制点中所有要求项的符合程度进行分析和判定。
- 安全控制点间安全测评是对同一区域同一类内的两个或者两个以上不同安全控制点间的关联进行测评分析,其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

- 区域间安全测评是对互连互通的不同区域之间的关联进行测评分析,其目的是确定这些关联对等级保护对象整体安全保护能力的影响。

（六）测评整改服务

依据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》、《GB/T 22080-2016 信息安全技术 信息安全管理体系要求》、《GB/T 22081-2016 信息安全技术 信息安全管理实用规则》《GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》等标准要求，对测评过程中发现的安全问题协助采购人进行安全整改，包括完善安全技术防护措施和安全管理制度，使得系统的整体安全防护水平基本满足等级保护要求。

（七）年度测评备案服务

测评结束后，向武汉市公安局提交我单位重要信息系统年度测评报告及其他所需资料，确保资料齐全、流程合规，满足武汉市公安局关于年度测评工作备案的要求。

（八）等级保护服务内容

项目	服务内容	工作描述
等级保护服务内容	项目准备及现场调研	进行现场调研，完成信息系统相关资料的收集和分析工作，准备好测评所需工具及表单。
	定级备案及年度测评备案服务	按照《GB/T22240-2020 信息安全技术 网络安全等级保护定级指南》等要求完成新增系统的定级备案工作，取得武汉市公安局颁发的备案证明。 按照武汉市公安局的要求提交我单位重要信息系统年度测评报告及其他所需资料，确保资料齐全、流程合规，顺利通过备案手续。
	差距测评服务	参照《GBT 22239-2019 信息安全技术 信息系统安全等级保护基本要求》和《GB T 28448-2019 信息安全技术 信息系统安全

		等级保护测评要求》等标准规范要求，开展差距测评服务，发现信息系统安全保护水平与标准之间的差距。
	等级保护安全整改	协助落实相关的等级保护建设整改工作，等级保护整改实施内容包括安全管理制度修订、安全技术整改、形成安全配置基线、进行安全增强配置、安全风险管理等，确保信息系统的安全防护能力满足国家等级保护标准的要求。
	二次测评服务	参照《GBT 22239-2019 信息安全技术 信息系统安全等级保护基本要求》和《GB T 28448-2019 信息安全技术 信息系统安全等级保护测评要求》等标准规范要求，针对差距测评中发现的安全问题的整改情况进行评估验证，在整改达到预期目标后出具符合要求的安全等级保护测评报告。
	成果	服务目标为通过公安部门的等级保护检查。 项目成果：《信息系统安全等级测评报告》

四、项目要求

（一）人员要求

1. 本项目实施人员必须具有丰富的工作经验且不得少于 4 人;测评人员必须具有等级保护测评师资质或注册信息安全员(CISM)证书，项目负责人应具有高级测评师资质（提供近半年社保证明）。

2. 投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有经验的测评人员进行本次等级保护测评工作。

（二）实施要求

1. 投标人应详细描述本次项目的整体实施方案，包括项目概述、技术方案、项目实施方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

2. 安全测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。

3. 投标人应提供针对本项目的工期要求和人员要求进行详细解读，提供详实、可行进度计划及保障措施。

4. 投标人应具有专业服务团队或攻防演练实验室平台，确保提供高效、精准的安全风险检测结果。

5. 投标人应具有良好的资信状况，提供企业资信等级证书和近一年财务审计报告。

（三）工具要求

1. 本项目实施和验收测试所需的工具，由投标人负责提供。用于测评的工具主要包括服务器安全测评工具、网络设备安全测评工具、终端计算机安全测评工具、网站等应用系统安全测评工具等。在使用前，应对工具进行测评，如果需要则对工具进行软件或代码升级。

2. 投标人须提供测评所使用工具的合同或证明文件。

（四）保密要求

1. 投标人必须和采购人签订保密协议，投标人必须要与参加此次项目的所有项目组成员签订保密协议，在合同签订时一并提供给采购人。

2. 投标人具体实施项目中的重要资料和结果，在项目实施期间和实施结束后，投标人不得带离该地点。

3. 投标人对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论投标人中标与否，其对上述内容的保密责任将长期存在。

4. 投标人应保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险。

5. 投标人应对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

（五）测评质量要求

项目管理是贯穿整个项目的一项任务。通过实施有效的项目管理，保证本项目能够按工作范围要求、按时间、按质量完成。投标人应提供质量控制及保证措施方案，包含项目质量控制及保证措施等。

（六）测评风险规避要求

项目开展工作涉及到单位重要信息系统和数据，在测评过程中必须加强安全保密管理与风险控制。

指定项目经理为专人负责信息安全测评过程中的安全保密管理工作，对测评活动、测评人员以及相关文档和数据进行安全保密管理，对重点设备的技术检测进行监督，对接入的检测设备进行控制。

安全测评工作中可能出现的安全风险点,按照检测对象周密制定测评方法，根据被测评对象的不同采取相应的风险控制手段。不限于以下方法：

1. 操作的申请和监护

在实施过程中必须遵守的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。

2. 操作时间控制

对测评直接影响系统工作时，尽可能避开敏感时期。

3. 人员与数据管理

必须高度重视信息保密工作，加强资料管理，确保人员可靠、稳定和可控。测评与被测评单位之间应签署长期保密协议，测评人员与被测评单位之间也要有相应的约束和控制措施，按国家有关要求做好保密工作。

4. 制定应急预案

根据测评范围界定的系统情况，在实施前制定应急预案。

5. 关键业务系统风险控制

对影响较大的重要关键业务系统在无法搭建模拟环境情况下，原则上不采用测评工具，采用访谈、测评和简单测试的方式进行。

6. 优化扫描策略

分类扫描:对不同的主机和设备类型执行不同的扫描会话，从而减少不必要的脆弱项目测试。针对扫描对象细化扫描策略：对不同类型的主机或设备，需要根据其上不同的应用和服务情况，有针对性地定制扫描策略选项。

7. 数据备份与恢复

对业务系统和数据库主机，应对其上数据进行备份，防止测评过程中对设备与主机的损伤影响业务系统的正常运行。

五、商务要求

1. 合同履行期限：合同签订生效、具备进场条件后，按照采购人要求分批次进行信息系统等级保护服务，出具测评报告，达到验收标准。

2. 验收标准：

中标人必须出具符合公安部门要求的《信息系统等级保护测评报告》。该项目过程中产生的文档，归采购人所有。中标人必须按照武汉市公安局的要求完成定级备案及年度测评备案手续。

3. 付款方式：

第一阶段：合同签订后，乙方向甲方开具相应金额的发票，甲方启动支付流程，在15个工作日内向乙方支付合同总价的35%。

第二阶段：乙方在提交27个系统《信息安全等级测评报告》后，向甲方开具相应金额的发票，甲方启动支付流程，向乙方支付合同总价的50%。

第三阶段：乙方在提交剩余4个系统的《信息安全等级测评报告》后，向甲方开具相应金额的发票，甲方启动支付流程，向乙方支付合同总价的15%。

4. 服务要求：

（1）投标人必须承诺提供 7*24 小时响应服务，1 小时到达现场。服务方式包括电话技术支持、远程技术支持、现场技术支持等。

（2）投标人在本地设有常驻机构（提供常驻机构或合作企业资料复印件、营业场所租赁或购买合同复印件、人员近半年社保证明资料等证明材料）。