武汉市第三医院网络安全等级保护
测评项目采购需求

第一章　供应商资格要求

1、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。

2、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；

3、必须具有公安部第三研究所认证发放的《网络安全等级测评与检测评估机构服务认证证书》。

4、应未被列入失信被执行人、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；

5、本项目不接受联合体投标

第二章 技术要求及商务要求

（一）测评服务及实施要求

1、测评服务目标

为做好网络安全保障工作，按照“全面排查风险、及时发现预警、快速有效处置、确保万无一失”的工作目标，确保关键敏感时期不发生网络安全事件，保障重要信息系统平稳运行。拟对重要系统开展等级保护测评工作，测评机构需要提供切实有效的整改方案、并提供整改咨询方案；对整改后的信息系统进行回归测评，最终达到国家等级保护相关要求。

2、服务内容及范围：

2.1 具体服务清单：

序号	系统名称	级别
1	HIS 系统	三级
2	PACS 系统	三级
3	EMR 系统	三级

4	互联网自助服务系统	三级
5	官方网站	二级
备注	具体系统名称以最终实际需求或网监部门备案名称为准。	

2.2 具体服务内容：

参照《GBT22239-2019 网络安全等级保护基本要求》和《GB/T28448-2019 网络安全等级保护测评要求》等标准规范要求，由具备等级测评资质或网络与信息安全管理员能力人员提供信息系统等级保护测评及整改指导工作。测评及整改范围为项目目标所涉及的基础网络环境、主机层面、应用层、数据库层及相关安全辅助设备与管理制度，服务目标为最终通过公安部门及相关部门的等级保护检查要求。

2.3 标准和规范

《GBT 20272—2006 信息安全技术 操作系统安全技术要求》

《GBT 20273—2006 信息安全技术 数据库管理系统安全技术要求》

《GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南》

《GBT 22239—2019 信息安全技术 网络安全等级保护基本要求》

《GB/T 25070—2019 信息安全技术 网络安全等级保护设计技术要求》

《GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求》

《信息安全等级保护管理办法》（公通字[2007]43 号文件）

《信息安全等级保护备案实施细则》（公信安[2007]1360 号）

2.4 实施原则

本项目实施方案设计与具体实施必须满足以下原则：

2.4.1 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招标方的行为。

2.4.2 标准性原则：测评方案的设计与实施应依据国家信息系统安全等级保护的相关标准进行。

2.4.3 规范性原则：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。

2.4.4 可控性原则：项目安排工作进度要跟上进度表的安排，保证工作的可控性。

2.4.5 最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能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。

2.4.6 整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

2.5 整体要求

2.5.1 供应商应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

2.5.2 供应商所提供参与本项目的测评人员的组成、资质及各自职责的划分（参与现场人员的

项目经理具备高级及以上测评资质或信息安全管理体系 ISO27001 主任审核员资质）。参与本项目测评人员不少于 5 人，应配置有中级测评资质或网络与信息安全管理员等专业人员进行本次工作。

2.5.3 供应商具备公安部第三研究所认证发放的《网络安全等级测评与检测评估机构服务认证证书》。

2.5.4 本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件由成交人推荐，经采购人确认后由成交人提供并在信息系统等级保护测评中使用。

2.5.5 信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由采购人提供，供应商应详细描述需要的运行环境的具体要求。

2.5.6 供应商必须具备项目所在地售后服务能力，出现安全事件能第一时间达到用户现场，要求售后服务团队成员不少于 15 人（需要提供近半年项目所在省的社保证明）。

2.6 专用工具要求

本项目涉及工程实施和验收测试所需的工具，由供应商负责提供。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。

2.7 安全管理要求

为做好全过程的安全保密工作，在等级保护测评前、中、后三个阶段都要做好安全保密工作。

2.7.1 等级保护测评前

2.7.1.1 对等级保护测评人员要进行安全保密教育，制定安全保密措施。

2.7.1.2 签订安全保密协议。

2.7.2 等级保护测评中

2.7.2.1 对被测单位的性质、机房物理位置、网络与系统、应用与服务、资料与数据、人员与管理等方面的信息进行严格的安全保密管理。

2.7.2.2 等级保护测评工具应经过严格测试和检验，确保不对被测评系统造成损失，工作结束后不驻留任何程序。

2.7.2.3 对被测单位信息系统的信息资产、发现的脆弱性和发生过的安全事件等威胁情况要控制知情范围。

2.7.2.4 对测评设备、介质进行严格的保密管理。

2.7.2.5 工作过程中对人员要实施封闭式集中管理.

2.7.2.6 对进场人员遵守被测单位的相关管理规定。

2.7.3 等级保护测评后

2.7.3.1 认真清退各种文档、资料和数据并予以销毁，确保工作过程中敏感数据不被泄漏。

2.7.3.2 现场工作结束后，按被测单位的要求及时还原系统，确保系统中不遗留任何代码或可执行程序。

2.7.3.3 在其他风险测评任务或宣传材料中不涉及被测单位的秘密、敏感情况。

2.8 文档要求

文档或报告的编写应完整清晰、用词规范、简明扼要，指出的问题应明确合理、符合逻辑、且有证据，出具的结论应公正客观、实事求是，提出的建议应符合国家标准规范、富有建设性和可操作性。

2.9 售后服务

供应商应承诺能按要求实现本技术规范规定的所有条款及功能要求，配合完成相关部门的信息安全等级保护相关（登记、整改等）工作要求。

（二）测评服务要求

根据国家等级保护相关标准，信息系统安全等级保护测评应包括以下内容：

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、安全管理中心等五个方面的安全测评；

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、安全建设管理、安全运维管理等五个方面的安全测评。

1、服务内容：

协助开展系统和重要信息系统的自查自评估工作，对存在的风险隐患和安全问题及时提供有针对性的安全整改建议，保障整改措施的落实，指导完成重要信息系统的定级、备案等相关工作；

依据《信息系统安全等级保护基本要求》，从安全技术和管理两个方面共十个层面对信息系统进行等级测评，出具等级测评报告。

针对信息系统等保测评实施过程中发现的安全隐患和薄弱环节，提供安全建设整改和安全加固方面的咨询。

提供国家和行业有关信息安全等级保护政策和标准方面的知识培训和安全管理咨询，增强信息安全意识。

项目	服务内容	工作描述
等级测评	项目准备及现场调研	协助对信息系统物理环境、网络、终端、数据、安全管理等进行调研。
	信息系统定级、备案	疏理信息系统定级工作，完成信息系统定级报告及定级材料的准备； 整理、补充信息系统备案所有相关的文档，指导用户方完成相应信息系统等级保护备案工作。 【备注：原则上已取得信息系统备案证明的系统不需要重新备案】
	信息系统差距分析	对定级的信息系统，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。

	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，等级保护整改实施具体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、辅助进行安全增强配置和调试指导工作等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。
	等级保护测评	参照《GBT22239-2019 网络安全等级保护基本要求》和《GB/T28448-2019 网络安全等级保护测评要求》等标准规范要求，对信息系统开展信息系统等级保护测评工作。
	成果	服务目标为通过公安部门的等级保护检查，输出《信息系统等级保护测评报告》。

1.1.1 安全物理环境

物理安全测评是对信息系统的机房和办公场所的物理位置选择、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、电磁防护等方面的安全状况。

1.1.2 安全通信网络

网络安全测评是对信息系统的网络系统安全防护情况进行测评，包括网络结构安全、网络访问控制、网络安全审计、网络边界完整性测评、网络入侵防范、网络恶意代码防范、网络设备防护等方面的安全状况。

1.1.3 安全区域边界

安全区域边界是对信息系统的边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的安全状况。

1.1.4 安全计算环境

安全计算环境是对信息系统的身份鉴别、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、数据备份恢复、剩余信息保护、个人信息保护等方面的安全状况。

1.1.5 安全管理中心

安全管理中心是对信息系统的系统管理、审计管理、安全管理、集中管控进行测评。

1.1.6 安全管理制度

安全管理制度测评是对信息系统的安全策略、管理制度、制定和发布、评审和修订等情况进行测评。

1.1.7 安全管理机构

安全管理机构测评是对信息系统的岗位设置、人员配备、授权与审批、沟通和合作、审核和检查等情况进行测评。

1.1.8 安全管理人员

人员安全管理测评是对信息系统相关内部人员的人员录用、人员离岗安全意识教育和培训、外

部人员访问管理等情况进行测评。

1.1.9 安全建设管理

系统建设管理测评是对信息系统建设过程中的、测试验收、系统交付、等级测评服务供应商管理等情况进行测评。

1.1.10 安全运维管理

系统运维管理测评是对信息系统运行维护过程中的环境管理、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、外包运维管理等情况进行测评。

2、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。项目经需理具备中级以上测评资质，具备丰富的等级保护测评经验。

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：

2.2.1 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。

2.2.2 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。

2.2.3 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。

2.2.4 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。

2.2.5 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。

2.2.6 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。

2.2.7 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。

2.2.8 厂商协作

厂商需要提供各应用系统的名称、版本、协议、开发语言、进程名和相应的端口号等信息，在测评之前，由三方共同分析测评对业务可能造成的风险，分析可能存在的问题。在测评过程中尽量规避这些风险。

3、整改实施内容

供应商严格按照差距分析报告内容，落实相关的等级保护建设整改指导工作，等级保护整改实施具体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、进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。

4、复评内容

供应商对差距分析报告中测评不通过的项目进行复测评，直至满足等级保护测评要求。

5、出具正式等级保护测评报告并通过公安机关认可，协助取得备案证明。

二、商务及其它要求

1、合同付款方式：合同中甲乙双方协商约定。

2、服务时间：项目具备测评条件之日起 60 个工作日内完成等级测评工作(网络安全建设整改不含在项目工期内)。

3、如成交供应商发生兼并、重组，由新组建的公司按投标文件承担相应售后服务；供应商使用的技术装备、设施应当符合《信息安全等级保护管理办法》中对信息安全产品的要求；

4、供应商的技术方案中应有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。

第三章 评分表

评标指标为报价、技术、服务和商务。其中报价部分 30 分，技术部分 35 分，商务 35 分。

评审因素		分值	评分标准
价格部分（30 分）		30	对于合格的投标报价，得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）×30%×100。 注：评标基准价为所有合格投标报价中的最低价，报价得分精确到小数点后两位；无效投标的报价不计入价格分值的计算。
技术部分（35 分）	安全服务方案	7	投标人按照项目服务内容提供的安全技术方案符合科学性原则，部署合理，切实可行。技术方案中提供明确的流程组织得 2 分，提供齐全的工具清单得 2 分、提供详细得风险控制措施 3 分，没有提供不得分。

	项目实施进度安排	7	投标人提供各项目实施进度、部署合理，可操作性强，实施方案中提供详细的测评计划得 3 分，提供齐全的项目进度保障措施得 4 分，没有提供或不合理不得分。
	质量保证措施	7	投标人提出得有效且合理得质量保证措施，提供完善的定级备案、测试、咨询评估、保障服务措施得 3 分，提供严谨的测评流程得 2 分，提供详细的测评指标得 2 分，其他不得分。
	合理化建议	7	针对本次项目的特点能在技术、实施及管理方面提出科学合理、有针对性的建议，提供合理化的测评流程得 3 分，提供合理化的整改建议得 4 分，没有提供不得分。
	技术能力	7	投标人技术能力具有中国合格评定国家认可委员会（CNAS）认证颁发的实验室认可证书，提供 CNAS 实验室证书资质得 7 分，没有提供不得分。（提供资质证明）
商务部分（35 分）	项目案例	4	按照以下要求提供项目所在省份、行业内相关的业绩(应为 2023 年 1 月 1 日以后签订)，需提供合同复印件。包括买卖双方名称及盖章、服务内容，每个业绩 1 分，最多得 4 分，否则不予认定加分。
	应急服务能力	12	为保障服务商安全应急响应能力，投标人拥有： 1.具备中国网络安全审查技术与认证中心出具的应急服务一级资质得 7 分（提供资质证书）； 2.拥有湖北省级网络安全应急服务支撑单位证书得 5 分。没有提供不得分（提供资质证明复印件）
	服务能力	7	投标人拟投入项目的服务团队，能够并提供承诺函： 1、承诺 40 分钟以内到现场处理应急工作，得 2 分（需提供交通线路图等证明材料）； 2、服务团队成员具备 20 名或及以上得 5 分，不足 20 人不得分（项目开标之日起倒推：提供人员近半年本地化社保证明材料）
	项目人员配备	12	投标人提供网络安全等级测评师（高级）且同时具备信息安全管理体系 ISO27001 主任审核员资质，得 6 分； 项目团队中，提供至少 3 名网络与信息安全管理员，每提供一名得 2 分，最高得 6 分。 评审依据：须提供以上人员对应的证书扫描件并加盖投标人公章，未提供或不符合要求不得分。