

第五章 采购需求书

1. 采购需求

序号	项目名称	单位	数量	核心服务内容
1	妇幼保健网络信息系统升级改造-第三方测评服务	项	1	对妇幼保健网络信息系统升级改造项目进行测评，整体工期预计≤6个月，测评工作分以下两阶段实施： 第一阶段：完成软件测试和安全测评的第一轮测试； 第二阶段：问题修改完成后，完成回归测试，如回归测试不通过须进行复测，直至测试通过后进行验收。

2. 项目背景

本项目源于北京市“三医”联动战略布局与妇幼健康服务升级需求。现有北京市妇幼保健网络信息系统存在技术架构陈旧、数据共享壁垒、公众服务能力不足等问题，难以满足1000余万妇女儿童日益增长的健康服务需求；同时也为推进健康北京建设，以信息化为驱动，实现以健康为中心的理念转变，满足群众多样化的需求，需要对北京市妇幼保健网络信息系统进行升级改造，通过升级改造北京市妇幼保健网络信息系统，构建覆盖全生命周期的智慧妇幼服务体系，推动妇幼健康服务数字化转型，采用集成、开放、服务的架构，完善及新增符合新政新规要求的妇幼核心业务模块，通过互联网模式为群众提供统一入口、多样化的妇幼健康服务，为北京市智慧妇幼健康新模式提供信息化的支撑措施。

3. 项目目标

为贯彻《中华人民共和国网络安全法》《国家政务信息化项目建设管理办法》等法律法规、规章制度以及国家有关标准的相关要求，拟向国内专业安全评估机构采购软件测评、安全测评等工作，对本次升级改造的项目在最终验收前完成软件测试和应用安全测评，为系统稳定运行提供质量保障，为系统验收提供客观依据

，确保北京市妇幼保健网络信息系统升级改造项目能够满足网络安全和用户使用要求。

3.1服务内容

序号	服务项	服务内容	单位	数量
1	软件测评	针对升级改造后的北京市妇幼保健网络信息系统开展软件测评工作，在升级改造项目终验之前出具软件测试报告，包括并不限于功能测试、性能效率测试、兼容性、易用性、可靠性、用户文档测试等方面测试，发现差距问题并开展回归测试。	项	1
2	安全测评	针对升级改造后的北京市妇幼保健网络信息系统进行安全功能测评，在升级改造项目终验之前出具相应测评报告。	项	1

4. 测试技术要求

4.1总体原则

方案设计与项目实施应满足以下原则：

- 公平原则：实施方应遵循“面向应用、保证质量、客观公正、诚信守诺”的原则开展安全评测工作。
- 标准性原则：实施方应依据相关国家标准、行业标准开展评测工作。本评测要求所使用的标准和规范如与实施方所执行的标准不一致时，按较高标准执行。
- 优质服务原则：本评测要求实施方提供的是最低限度的要求，实施方应保证提供符合本评测要求和有关标准的优质服务，并确保评测报告符合项目最终验收的所有要求。
- 保密原则：对评测服务过程中接触到的各种信息，不得泄漏给任何单位和个人，未经允许不得利用这些信息从事与服务无关的活动。

4.2测试依据

需遵循的标准包括但不限于如下：

GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

《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）

《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）

《信息安全等级保护管理办法》（公通字[2007]43号）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

4.3 测试范围

测试的范围为北京市妇幼保健网络信息系统升级改造项目所有模块（包含平台端和移动端）的软件测试和应用系统安全测评。

4.4 软件测试要求

软件测试内容包括功能测试、性能效率测试、兼容性、易用性、可靠性、用户文档测试等方面。通过测试了解所交付的软件系统的是否就绪可用，是否达到质量要求，是否实现项目申报所描述的交付要求。软件测试内容如下：

（1）功能性测试应按照业务需求严格对软件功能模块、业务流程、界面等进行全方位的测试，对本项目所有业务软件功能表现的准确性、一致性、互操作性进行验证，确保业务功能符合实际业务运行需要，满足采购方要求。

（2）性能效率测试应对应用软件的时间特性、资源特性等进行测试，包括但不限于并发用户、响应时间、负载量、吞吐量、资源利用率、事务通过率等是否与用户文档集中的相应描述一致进行测试。

（3）可靠性测试应测试各业务系统在各种条件下使用时，系统各功能操作的成熟性、容错性、宕机时间易恢复性、数据检验机制等。

（4）易用性测试应对应用软件的易理解性、易浏览性、易操作性、易分析性、易改变性、稳定性进行测试，测试是否有可被修改的能力。

(5) 兼容性测试应包括易安装性、适应性、易替换性、共存性、互操作性测试，就产品说明中列出的所有支持平台和系统加以验证。

(6) 用户文档测试内容应包括文档的完整性、完备性、正确性、一致性、易理解程度、易浏览程度、易学性、可操作性的检查和验证，验证软件文档与软件程序之间的一致性。

4.5应用系统安全测评

验证待测系统的安全机制是否符合国家信息安全等级保护三级标准，确保系统不存在安全漏洞，尤其是针对数据泄露、未授权访问、恶意攻击等风险。具体内容如下：

(1) 身份鉴别：

- 1) 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。
- 2) 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。
- 3) 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。
- 4) 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。

(2) 访问控制：

- 1) 应对登录的用户分配账户和权限。
- 2) 应重命名或删除默认账户、修改默认账户的默认口令。
- 3) 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。
- 4) 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。
- 5) 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。
- 6) 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。
- 7) 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。

(3) 安全审计：

- 1) 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
- 2) 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
- 3) 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
- 4) 应对审计进程进行保护，防止未经授权的中断

(4) 入侵防范

- 1) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
- 2) 应关闭不需要的系统服务、默认共享和高危端口；
- 3) 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；
- 4) 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；
- 5) 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；
- 6) 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。

(5) 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。

(6) 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。

(7) 数据完整性

- 1) 应采用校验技术或密码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。

- 2) 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。

(8) 数据保密性:

- 1) 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。
- 2) 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。

(9) 数据备份恢复

- 1) 应提供重要数据的本地数据备份与恢复功能;
- 2) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地;

(10) 剩余信息保护

- 1) 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全清除;
- 2) 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。

(11) 个人信息保护:

- 1) 应仅采集和保存业务必需的用户个人信息;
- 2) 应禁止未经授权访问和非法使用用户个人信息。

5. 项目管理及服务要求

5.1. 服务保证

应严格执行项目管理规定，从项目组织管理、项目进度管理、项目质量保障和安全保密等方面加强项目管理，确保服务质量。

5.2. 质量保证

应建立严格的质量保证体系，制定项目建设的质量控制方案和实施措施，并督促落实各环节质量控制内容和目标;保证项目各个阶段工作满足采购人对质量的要求。应根据项目的工作计划，对阶段性工作成果进行审核，并向采购人提交里程碑式工作成果。通过保证各阶段性成果的质量，最终保证整个项目的质量。

5.3. 工期保证

- (1) 在本项目合同签订之后，按合同约定完成相关工作。
- (2) 项目进度管理应该遵循以下原则:

1) 项目进度管理的依据是项目合同所约定的工期目标；

2) 在确保项目质量和安全的原则下，控制项目进度。

(3) 项目进度管理应该至少包含以下内容：

在了解项目详细情况后，按照合同约定工期制定具体实施计划，明确各阶段工作任务；

按照具体实施计划，定期跟踪检查，对可能发生的延误提出相应对策；定期或不定期地召开或参加项目例会、协调会议等，向采购人通报项目进展情况，提交进度报告，及时解决相关问题。

6. 测试实施要求

(1) 投标人应按照采购人的要求制定详细的项目实施计划，在项目实施计划由采购人确定后，投标人进入实施阶段。

(2) 投标人应依据项目合同和项目进度安排确定测试内容和测试关键点，制定详细的测试计划和测试方案，设计测试用例，并经采购人确定后进入具体测试实施阶段。

(3) 投标人应依据合同条款及相关标准分阶段向采购人提交测试文档。

(4) 投标人应在测试过程中，制定缺陷管理方案，并及时向采购人提交缺陷报告。对调整后的系统提供回归测试直至通过测试为止。

(5) 投标人应按采购人要求提交第三方测试报告，该报告的内容包括测试结论、详细测试结果描述以及软件的测试环境描述等。

(6) 投标人应成立合理的组织机构，严格按照项目管理制度保证测试工作按质、按量、按时实施。

7. 团队人员要求

(1) 投标人应组织一个专业化的团队来执行本项目。

(2) 该团队需指定项目经理1名，负责项目整体统筹与全流程管理，把控进度、质量、风险及交付验收；审核测评方案、测试用例及测试报告，对交付成果质量负责；

协调内外部资源，确保测评各环节合规有序推进；具备10年以上测评相关工作经验，能有效应对各类复杂问题。

(3) 投标人需指定技术负责人1名，负责测试方案设计与评审，确保测评方法科学、工具适用、路径合理，对测试结果的准确性负责；从系统架构和

安全视角全面把控测评深度与覆盖范围；具备5年以上测评技术经验，能快速定位并解决技术问题。

(4) 投标人需指派具体负责测试工作的人员不少于4人，负责具体测评执行工作，包括测试用例编制与执行、结果记录、文档编写等。

8. 测试环境要求

(1) 采购人提供被测试的应用系统安全测试环境。如果是生产环境投标人必须给出合理的使用计划，该计划不会对生产环境造成任何影响。

(2) 投标人必须在投标文件中详细说明用于本次测试的测试内容、测试方法、测试工具及其使用计划。

投标人应对测试过程中使用的各种软件的版权负责。如果因此引起版权纠纷，由投标人承担相应责任。

9. 测试工具要求

为保证测试的公正和准确，为本项目测试所采用的测试工具均需为专用测试工具，并且在投标文件中需写出具体的工具介绍和使用计划。

10. 保密要求

(1) 投标人应与采购人签订保密协议或条款。如果参与测试的人员在规定的保密期内发生失泄密行为，投标人应承担全部责任。项目实施过程中，中标单位所收集、产生的所有与本项目相关文档、资料，包括文字、图片、表格、数字等各种形式所属权均归属甲方，中标单位有义务对所涉及到的内容保密，中标单位须按照采购人的要求签署保密协议。

(2) 投标人必须在投标文件中对测试过程中引用或产生的所有资料做出明确的保密承诺，包括但不限于纸质文档、电子文档、数据、软件、程序、用户名、口令和资料等。

(3) 在未经采购人书面同意的情况下，投标人不得将本项目、与项目中相关的任何内容、资料（包括所涉及的书面和磁介质资料，下同）透露给任何人。中标单位如违反安全保密条款，采购人将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任。对中标单位泄露采购人资料，造成伤害的，除依据国家法律有关规定追究有关责任人员法律责任外，还将依法承担相应的责任。

11. 售后服务

应建立统一的售后技术支撑服务体系，能够提供项目测试工作后续建议的跟踪、其他与项目测试相关的工作事项。

12. 服务期限

自具备测评条件之日起45天内完成。

13. 验收要求

在合同约定的最终交付日期，投标人完成合同约定的全部工作内容并提交验收申请后，由采购人组织专家对整体服务项目进行验收。

验收交付成果为：

《北京市妇幼保健网络信息系统软件测试问题报告》

《北京市妇幼保健网络信息系统安全测试问题报告》

《北京市妇幼保健网络信息系统软件测试报告》，加盖CNAS章

《北京市妇幼保健网络信息系统安全测试报告》，加盖CNAS章

《项目实施方案》