第五章　采购需求

1. 项目概述

1.1. 采购需求

序号	项目名称	单位	数量	工期
1	妇保院中央转移支付 2023 年医疗卫生机构能力建设项目-软件测评子项	项	1	妇保院中央转移支付 2023 年医疗卫生机构能力建设项目（简称“建设项目”）整体工期为10个月。 第一阶段：完成软件测试、源代码审计和网络安全等级保护测评的第一轮测试； 第二阶段：问题修改完成后，进行回归测试，回归测试一轮，经测试通过，进行验收。

1.2. 项目背景

2021年，由北京市卫生健康委牵头、北京妇幼保健院（首都医科大学附属北京妇幼保健院）负责承建完成了国家“云上妇幼”远程医疗平台（北京市）一期的建设，通过远程教学、远程培训、远程会诊和指导、妇女健康公众服务等基本功能的建设，建立起了与下级医疗机构连接的远程医疗信息系统和工作机制，开展北京市妇幼健康“大手拉小手”行动，促进妇幼健康优质医疗资源下沉基层。

为进一步推进省域妇幼健康“大手拉小手”行动，规范省级“云上妇幼”远程医疗平台建设和应用，将依据《关于下达2023年医疗服务与保障能力提升（医疗卫生机构能力建设)补助资金预算的通知》(财社[2023]33号)、《国家卫生健康委妇幼司关于做好2023年妇幼保健机构能力建设项目工作的通知》（国卫妇幼妇卫

便函[2023]14号）、《中国疾病预防控制中心妇幼保健中心 关于推进2023年妇幼保健机构能力建设项目相关配套文件的通知》（中疾控妇孕便函[2023]36号）要求，北京市继续组织实施妇幼保健机构能力建设项目。北京市根据实际情况制定《北京市2023年妇幼保健机构能力建设项目实施方案》，在完成“云上妇幼”远程医疗平台2022年建设任务的基础上，进一步推进实化细化优化远程医疗平台的基本功能模块。

2. 项目目标

本次第三方测试服务项目的总体工作目标是：在项目预验收前完成软件测试，项目验收前完成源代码审计和网络安全等级保护（三级等保）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，确保妇保院中央转移支付 2023年医疗卫生机构能力建设项目能够满足用户使用要求。妇保院中央转移支付2023 年医疗卫生机构能力建设项目即国家“云上妇幼”远程医疗平台（北京市）的升级改造项目。

3. 第三方测试技术规格

3.1. 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。

3.2. 测试依据

需遵循的相关标准包括：

- 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
- GB/T 15532-2008 计算机软件测试规范
- 《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）
- GB/T 39412-2020 《信息安全技术 代码安全审计规范》
- 《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 网络安全等级保护测评过程指南》(GB/T 28449—2018）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

3.3. 测试范围

测试的范围为国家“云上妇幼”远程医疗平台（北京市）(包括平台端及所涉及的小程序）的软件测试、源代码审计和网络安全等级保护（三级等保）测评。

3.4. 软件测试要求

3.4.1. 软件测试内容

（1）功能性测试：

- 登录与退出
- 功能表现
- 正确性
- 一致性

（2）性能效率测试：

- 时间特性
- 资源特性

（3）易用性测试：

- 易理解性
- 易浏览性
- 易操作性

（4）可靠性测试：

- 成熟性
- 容错性
- 易恢复性
- 数据检验机制

（5）兼容性测试：

- 共存性
- 互操作性

（6）用户文档测试：

- 完整性
- 正确性
- 一致性
- 易理解程度
- 易浏览程度

3.4.2. 交付成果

《妇保院中央转移支付2023年医疗卫生机构能力建设项目验收报告》

3.5. 源代码审计测评要求

3.5.1. 源代码审计测评内容

依据GB/T 39412-2020 《信息安全技术 代码安全审计规范》、参考CWE（Common Weakness Enumeration通用缺陷列表）V4.6的要求进行源代码审计测评。

具体测试内容包括：输入验证与表示、API滥用、安全特性、时间与状态、错误处理、代码封装、代码质量和环境配置。

3.5.2. 交付成果

《妇保院中央转移支付2023年医疗卫生机构能力建设项目源代码安全测评报告》

3.6. 网络安全等级保护测试要求

3.6.1. 信息系统差距分析服务

信息系统安全等级保护差距分析将根据《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护测评过程指南》等标准文件的要求，对已定级信息系统，进行系统现状调研，逐项进行合规性检测。其实质是采用基线安全分析的方法，明确当前信息系统与等级保护要求的不符合项及差距。依据信息系统定级情况，对信息系统的各项安全指标进行符合性评估，标识信息系统的不符合项，明确信息系统与等级保护基本要求之间的差距。

- 根据项目的总体要求及信息系统等级保护体系建设现状需要，对信息系统进行差距分析，从安全技术差距分析测评和安全管理差距分析测评两部分进行，对系统各项安全指标进行符合性评估，并标识系统不符合项，明确系统与国家安全等级保护相关标准要求的差距。

- **交付成果**

《信息系统差距分析报告》

3.6.2. 信息系统整改咨询服务

信息系统安全建设整改咨询主要是依据差距分析报告，对被测信息系统面临的安全风险进行总结分析，对信息系统不符合信息系统等级保护建设基本要求的部分提供可行性整改建议或方案，从整体上把控内容，主要从技术和管理两方面进行整改，最终能够使被测信息系统在进行安全建设整改后可通过等级保护测评。

- **交付成果**

《信息系统安全整改建议书》

3.6.3. 信息系统等级保护测评服务

依据GB/T 28448-2019《信息安全技术网络安全等级保护测评要求》、GB/T22239-2019《信息安全技术网络安全等级保护基本要求》对妇保院中央转移支付 2023 年医疗卫生机构能力建设项目进行正式的信息安全等级保护测评及复测评，出具公安部门认可的网络安全等级测评报告。信息系统安全等级测评主要检测和评估信息系统在安全技术、安全管理等方面是否符合已确定的安全等级三级的要求，对于尚未符合要求的信息系统，分析和评估其潜在威胁、薄弱环节以及现有安全防护措施，综合考虑信息系统的重要性和面临的安全威胁等因素，提出相应的整改建议，最终用户根据初次等级保护测评工作中发现的问题进行整改，待整改工作结束后，进行等级保护复测确认，以确保信息系统的安全保护措施符合相应安全等级三级的基本要求，并提交符合国家等级保护测评三级要求的等级保护测评报告。

●交付成果

《妇保院中央转移支付 2023 年医疗卫生机构能力建设项目网络安全等级保护测评报告》**（测评完成后提交加盖检测专用章并符合公安部门安全等级保护要求的测评报告）**

4. 项目管理及服务要求

4.1. 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。

4.2. 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招标方对质量的要求。应根据项目的工作计划，对阶段性工作成果进行审核，并向项目单位提

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。

4.3. 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：

- 项目进度管理的依据是项目合同所约定的工期目标；
- 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，向招标方通报项目进展情况，提交进度报告，及时解决相关问题；

5. 测试实施要求

- 投标人应按照采购人的要求制定详细的项目实施计划（包括时间计划（包括测试周期）、实施地点等），在项目实施计划由采购人确定后，投标人进入实施阶段。
- 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，并经用采购人确定后进入具体测试实施阶段。
- 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。
- 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。
- 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。
- 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。

6. 测试人员要求

（1）投标人应组织一个专业化的团队来执行本项目。

（2）该团队需具备有经验的测试工程师，充分理解应用系统需求；熟悉软件测试；具有相应的信息技术软件检测基础理论的专业知识；接受过软件、硬件和网络技术等方面的技术培训；接受过知识产权保护方面的专门教育，具备知识产权意识，确保采购人利益和机密不被泄漏。

（3）投标人需指定一名项目总负责人，全程负责本项目测试工作。项目总负责人必须具有5年以上的信息系统测评工作经验，具有系统分析师（高级）、软件测试类高级工程师、网络安全等级测评师证书(均需相关提供证明)。

（4）投标人需指派具有3年以上软件开发和测试工作经验（其中1年以上的软件测试工作经验）的人员至少3人，承担项目重要岗位的工作。

7. 测试环境要求

- 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。
- 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。

8. 测试工具要求

为保证测试的公正和准确，测试所采用的测试工具均需为第三方测试工具，并且在投标文件中需写出具体的工具介绍和使用计划。

9. 保密要求

- 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，中标单位需按照甲方要求签署保密协议。

- 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、程序等。

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；对中标单位泄露甲方资料，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。投标人必须在对外保密的前提下，对从事本项目的投标人员提供有关情况，所提供的情况仅限于执行投标必不可少的范围。

10. 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。