第四包

第五章　采购需求

第一部分

一、采购标的需实现的功能或者目标，以及为落实政府采购政策需满足的要求：

1、采购标的需实现的功能或者目标：投标人应根据招标文件所提出的采购需求，制定信息化与安全运维项目的具体服务方案，确保服务质量符合要求，以优良的服务和优惠的价格，充分显示自己的竞争实力。

2、为落实政府采购政策需满足的要求：

2.1、执行《政府采购促进中小企业发展管理办法》（财库[2020]46号）、《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库【2014】68号）、《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库【2017】141号）的相关规定，对小型和微型企业、监狱企业、残疾人福利性单位的价格给予10%的扣除，用扣除后的价格参与评审。

2.2、执行《财政部关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的相关规定，在评标时予以优先采购。

2.3、执行《关于开展政府采购信用担保试点工作的通知》（财库【2011】124号）的相关规定，接受投标人采用政府采购信用担保形式支付投标保证金及履约保证金。

二、采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范：符合已颁布的现行中华人民共和国认可的国家标准、地方标准和行业标准。如果这些标准内容有矛盾时，应按最高标准的条款执行。

三、采购标的需满足的质量、安全、技术规格、物理特性等要求：详见第二部分

四、采购标的交付或者实施的时间和地点：

采购标的实施时间：2年

采购标的实施地点：北京市疾病预防控制中心

五、采购标的需满足的服务标准、期限、效率等要求：详见第二部分

六、采购标的的验收标准：详见合同条款

七、采购标的的其他技术、服务等要求：

1、投标单位须提供满足招标文件第五章“服务需求”章节中各项要求及服务方案。

2、投标单位的投标文件应包括独立的服务承诺章节，将所有服务承诺明确列出。

3、投标单位提供纸质盖章承诺书，承诺按照本次投标方案提供的人员、团队作为驻场人员和服务团队签合同，且保证投标方案提供的驻场人员在合同有效期前3个月内不得更换。

第二部分

1. 项目背景

北京市传染病智慧化多点触发监测预警平台项目包含北京市传染病智慧化多点触发监测预警平台系统和智能流行病学调查系统以及与其他多方面系统的集成工作，系统的建设离不开软件的测评工作，软件测评工作的开展是保障本项目能最终验收的必要环节。

2. 项目目标

完成北京市传染病智慧化多点触发监测预警平台项目中涉及到的所有软件部分工作的测评工作，确保项目的最终验收，符合国家关于软件测评的规范要求，保障项目最终顺利验收。

3. 第三方测试技术规格

完成项目建设涉及的信息系统的软件验收测试。具体要求为：

3.1. 测试要求总则

3.1.1. 投标人应遵循“面向应用、保证质量、客观公正、诚信守诺”的原则，并依据相关国家标准、行业标准开展第三方测试工作。

3.1.2. 本测试要求提供的是最低限度的要求，投标人应保证提供符合本测试要求和有关标准的优质服务。

3.1.3. 本测试要求所使用的标准和规范如与投标人所执行的标准不一致时，按较高标准执行。

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 16260-2006 软件工程　产品质量
- GB/T 15532-2008 计算机软件测试规范
- GB/T 18905-2002　软件工程　产品评价
- GB 9386-2008 计算机软件测试文档编制规范

3.2. 软件验收测试要求

测试的范围主要包括：

- 北京市传染病智慧化多点触发监测预警平台系统（包含各子系统）
- 智能流行病学调查系统
- 统一系统集成（各系统之间集成对接测试）

测试内容具体要求如下：

（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）可移植性测试：

✓ 适应性

✓ 易替换性

（7）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

4. 测试实施要求

➢ 投标方应按照管理方的要求制定详细的项目实施计划（包括时间计划、实施地点等），在项目实施计划由管理方确定后，投标方进入实施阶段。

➢ 投标方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，并经用户方确定后进入具体测试实施阶段。

➢ 投标方应依据合同条款及相关标准分阶段向用户方提交测试文档。

➢ 投标方应在测试过程中，制定缺陷管理方案，并及时向管理方和用户方提交缺陷报告。对调整后的系统提供回归测试。

➢ 投标方应按管理方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。

5. 测试人员要求

5.1. 投标方应组织一个专业化的团队来执行本项目，并向管理方提供拟参与本项目的各人员的有效联系方式（包括手机、办公电话、传真、电子邮箱等）。

5.2. 该团队须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，确保招标人利益和机密不被泄漏。

5.3. 投标方须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 8 年以上的测试工作经验，4 个以上类似规模软件的测试工作经验和测试项目管理经验。出具人员从业简历、资质和聘任证明以及社保证明。

5.4. 投标方必须指派具有 3 年以上软件开发和测试工作经验（其中 2 年以上的软件测试工作经验）的人员全时承担项目重要岗位（质量审核、功能测试人员、性能测试人员）的工作并出具提供人员从业简历和聘任证明以及社保证明。

5.5. 测试团队一经创建，不得随意变更。未经管理方许可，项目总负责人不得变更并出具承诺函。

5.6. 项目团队具有相关机构颁发的软件评测类资格证书，例如：软件评测师、软件测评师、软件性能测试工程师、软件评测工程师或软件评测高级工程师等（提供资质证明复印件）。

6. 测试环境要求

- 招标方提供被测试的应用系统软件测试环境。如果是生产环境投标方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。
- 投标方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。
- 投标方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，由投标方承担相应责任。

7. 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，并且在应答文件中需写出具体的工具介绍和使用计划。

8. 保密要求

- 投标方应与委托方签订保密协议。如果参与测试的人员在规定的保密期内发生失泄密行为，投标方应承担全部责任。
- 投标方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。保密责任最终以正式签署的保密协议为准。

在未经采购人书面同意的情况下，投标方不得将本项目、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。否则，投标方必须承担因此给采购人造成的一切经济损失，采购人保留追究法律责任的权力。投标方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。

9. 进度要求

系统上线后六个月内完成。

第五包

第五章　采购需求

第一部分

一、采购标的需实现的功能或者目标，以及为落实政府采购政策需满足的要求：

1、采购标的需实现的功能或者目标：投标人应根据招标文件所提出的采购需求，制定信息化与安全运维项目的具体服务方案，确保服务质量符合要求，以优良的服务和优惠的价格，充分显示自己的竞争实力。

2、为落实政府采购政策需满足的要求：

2.1、执行《政府采购促进中小企业发展管理办法》（财库[2020]46号）、《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库【2014】68号）、《三部门联合发布关于促进残疾人就业政府采购政策的通知》（财库【2017】141号）的相关规定，对小型和微型企业、监狱企业、残疾人福利性单位的价格给予10%的扣除，用扣除后的价格参与评审。

2.2、执行《财政部关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的相关规定，在评标时予以优先采购。

2.3、执行《关于开展政府采购信用担保试点工作的通知》（财库【2011】124号）的相关规定，接受投标人采用政府采购信用担保形式支付投标保证金及履约保证金。

二、采购标的需执行的国家相关标准、行业标准、地方标准或者其他标准、规范：符合已颁布的现行中华人民共和国认可的国家标准、地方标准和行业标准。如果这些标准内容有矛盾时，应按最高标准的条款执行。

三、采购标的需满足的质量、安全、技术规格、物理特性等要求：详见第二部分

四、采购标的交付或者实施的时间和地点：

采购标的实施时间：2年

采购标的实施地点：北京市疾病预防控制中心

五、采购标的需满足的服务标准、期限、效率等要求：详见第二部分

六、采购标的的验收标准：详见合同条款

七、采购标的的其他技术、服务等要求：

1、投标单位须提供满足招标文件第五章“服务需求”章节中各项要求及服务方案。

2、投标单位的投标文件应包括独立的服务承诺章节，将所有服务承诺明确列出。

3、投标单位提供纸质盖章承诺书，承诺按照本次投标方案提供的人员、团队作为驻场人员和服务团队签合同，且保证投标方案提供的驻场人员在合同有效期前3个月内不得更换。

第二部分

10. 项目背景

北京市传染病智慧化多点触发监测预警平台项目包含北京市传染病智慧化多点触发监测预警平台系统和智能流行病学调查系统以及与其他多方面系统的集成工作，系统中涉及到公卫、医疗、个案等敏感信息，系统的建设离不开安全测评工作，系统需要达到等保三级要求，安全测评工作的开展是保障本项目能最终验收的必要环节。

1. 项目目标

完成北京市传染病智慧化多点触发监测预警平台项目涉及的信息系统安全测评工作，符合国家关于安全测评的规范要求，保障项目最终顺利验收。

2. 安全测试技术规格

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 28448-2019 信息安全技术 网络安全等级保护测评要求》等相关标准，开展安全测评/等级保护安全合规性检查工作包括：通用要求中安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面，以及云计算安全测评扩展要求、移动互联网安全测评扩展要求、物联网安全测评扩展要求、工业控制系统安全测评扩展要求等。投标人采取包括但不限于网络安全风险评估、等保差距分析、渗透测试、源代码审计等手段，对招标人信息系统进行技术检查和合规评审，并根据《网络安全等级保护测评报告模板（2021 版）》进行测评及分析，出具网络安全等级测评报告、安全合规性检查报告。投标人投标人按照 GB/T 22240-2020 《信息安全技术网络安全等级保护定级指南》等相关标准，协助投标人完成信息系统网络安全等级保护定级、备案工作。需完成工作包括不限于：根据对业务系统的梳理，协助整理出最终需要定级备案系统，指导定级备案的相关材料准备，并对定级备案材料进行审核（包括《定级备案表》、《定级报告》相关材料），负责组织召开定

级专家评审会。

3. 等级保护定级备案技术要求

为进一步贯彻落实《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》(国务院令第147号)、《国家信息化领导小组关于加强信息安全保障工作的意见》和公安部、国家保密局、国家密码管理局、国务院信息化工作办公室《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》(以下简称《管理办法》)、《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》等相关政策要求文件，依据《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》等相关技术标准要求，开展定级备案工作，提高基础信息网络和重要信息系统的信息安全保护能力和水平。

信息系统定级应按照自主定级、专家评审、主管部门审批、公安机关审核的流程进行。信息系统运营使用单位按照《信息安全等级保护管理办法》(以下简称《管理办法》)、《GB/T 22240-2020信息安全技术 网络安全等级保护定级指南》，自主确定信息系统的安全保护等级。为保证信息系统定级准确，需组织专家进行评审。有上级主管部门的，应当经上级主管部门审批，跨省或全国统一联网运行的信息系统可以有其主管部门统一确定安全保护等级。最后经公安机关审核把关，合理确定信息系统安全保护等级并核发备案证明。

4. 等级保护测评要求

5.1. 等级保护测评方法要求

等级保护测评过程中采用的测评方法应包含但不限于以下方法。

5.1.1. 访谈

访谈是指测评人员与被测评组织内的有关人员就测评所关注的问题进行有针对性的询问和交流的过程，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

访谈深度（即访谈内容的详细程度）以及访谈的广度（即对被测评组织中员工角色类型以及每种类型中人数的覆盖程度）由测评人员依据不同的测评需要进行选择和判断。

5.1.2. 核查

核查是测评人员通过对测评对象（如制度文档、各类设备及相关安全配置等）进行观察、查验和分析，以帮助测评人员理解、澄清或取得证据的过程。

比较典型的核查行为应包括：对安全配置的核查、对安全策略的分析和评审等。

5.1.3. 测评

测评是测评人员使用预定的方法／工具使测评对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行比对的过程。

5.2. 等级保护测评内容要求

5.2.1. 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、安全管理中心。

安全物理环境：安全物理环境测评应包含对物理位置的选择、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、电磁防护十个控制点，且通过访谈、文档审查和实地查看的方式测评信息系统的物理安全保障情况。主要涉及对象应为信息机房。

安全通信网络：安全通信网络测评应包含网络架构、通信传输、可信验证三个控制点，且通过访谈、配置检查、测试的方式测评信息系统的网络安全保障情况。主要涉及对象应包含网络互连设备、网络安全设备和网络拓扑结构等三大类对象。

安全区域边界：安全区域边界测评应包含边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证六个控制点，且通过访谈、配置检查、测试的方式测评信息系统的边界区域防护情况。主要涉及对象应包含边界设备等。

安全计算环境：安全计算环境测评应包含身份鉴别、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、个人信息保护十一个控制点，且通过访谈、配置检查、测试的方式测评信息系统的计算环境的安全保障情况。重点测评的对象包括服务器（各网站服务器、应用服务器和数据库服务器）、网络安全设备、应用系统、中间件、数据等。

安全管理中心：安全管理中心测评应包含系统管理、审计管理、安全管理、集中管控四个控制点，且通过访谈、配置核查的方式测评信息系统通过技术手段实现集中管理的情况。重点测评的对象为提供集中系统管理功能的系统、提供集中审计功能的系统、提供集中安全管理功能的系统等。

5.2.2. 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。

安全管理制度：安全管理制度测评应包含安全策略、管理制度、制定与发布、评审和修订四个控制点，且采用人员访谈与资料查阅的方式进行测评。

安全管理机构：安全管理机构测评应包含岗位设置、人员配备、授权和审批、沟通与合作、审核与检查五个控制点，且采用人员访谈与资料查阅的方式进行测评。

安全管理人员：安全管理人员测评应包含人员录用、人员离岗、安全意识教育和培训、外部人员访问管理四个控制点，且采用人员访谈与资料查阅的方式进行测评。

安全建设管理：安全建设管理测评应包含定级和备案、安全方案设计、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、投标人选择九个控制点，且采用人员访谈与资料查阅的方式进行测评。

安全运维管理：安全运维管理测评应包含环境管理、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、恶意代码防护管理、配置管理、密码管理、变更管理、备份和恢复管理、安全事件处置、应急预案管理、外包运维管理十四个控制点，且采用人员访谈与资料查阅的方式进行测评。

5.2.3. 安全测评扩展要求

如被测评系统采用云计算、移动互联等新技术，则在等保测评过程中要采用和相关等级保护基本要求中的相关扩展要求进行测评工作。

5.2.4. 安全验证性测评工作

包括系统漏洞扫描测评、渗透性测试等；

系统漏洞扫描测评：应对系统涉及的对象进行科学完备的漏洞扫描。漏洞扫描应使用业界领先的漏洞评估工具对评估范围内的主机和网络设备进行评估，从而对被评估的设备存在的漏洞有一个清晰的认识。

渗透性测试：渗透性测试应包含远程渗透测试和现场渗透测试。通过安全渗透测试，对系统的安全状况进行模拟攻击测试，挖掘可能存在的安全漏洞，并针对评估发现的安全问题以及合规要求，提供相应的渗透测试安全加固建议，协助公司完成漏洞修复，及时修补安全隐患。测试内容包括但不限于以下方面：暴力攻击，认证不充分，授权不充分等；命令执行类，包括 SQL 注入，操作系统命令，缓冲区溢

出等；逻辑攻击类，包括拒绝服务，跨站点脚本编制，客户端攻击等；信息泄露类，包括目录索引，路径遍历，信息泄露等方面。测试人员可以利用所有可用的资料和手段来企图绕开被测评项目的安全特性。

5.2.5. 整体测评分析

等级保护对象整体测评应从安全控制点、安全控制点间和区域间等方面进行测评和综合安全分析，从而给出等级测评结论。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。

安全控制点测评：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：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：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。

5.2.6. 系统安全保障评估

综合单项测评和整体测评结果，计算修正后的安全控制点得分和层面得分，并根据得分情况对测评系统的安全保障情况进行总体评价。

5.2.7. 安全问题风险分析

根据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对测评系统安全造成的影响。

5.2.8. 等级测评结论形成

找出系统保护现状与《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》标准之间的差距，并形成等级测评结论。

5.2.9. 安全整改建议

针对信息系统测评情况，根据测评结果，立足现有环境，对信息系统的安全整改及加固给出可操作和可实施的加固建议，并协助整改方案设计。

5.2.10. 报告编写

按照《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）的要求，结合招标人本次定级备案的信息系统的状况和信息系统安全保护等级的相应等级指标，通过

单项结果判定、单元结果判定、安全控制间分析、层面间分析和区域间分析、风险分析等一系列分析判定，得出被测信息系统的安全保护能力与标准要求的安全保护能力的符合性评价，按照《等级测评报告模板 2021 版》报告要求，针对被测系统编写并提交《网络安全等级保护测评报告》。

5. 项目组成员要求

- 投标方应组织一个专业化的团队来执行本项目，并向管理方提供拟参与本项目的各人员的有效联系方式（包括手机、办公电话、传真、电子邮箱等）。
- 该团队须具备有经验的等保测评师团队，充分理解应用系统安全现状；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，确保招标人利益和机密不被泄漏。
- 投标方须组建不少于 8 人的项目实施团队。
- 。
- 投标方必须指派具有 3 年以上等级保护测评工作经验（的人员全时承担项目重要岗位的工作。
- 团队一经创建，不得随意变更。未经管理方许可，项目总负责人不得变更。
- 项目团队均需具备等级保护测评师资质证明并提供中国等保网（www.djbh.net）上的单位情况和测评师公示截图。（提供资质证明复印件）。

6. 测试环境要求

- 招标方提供被测试的应用系统软件测试环境。如果是生产环境投标方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。
- 投标方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。
- 投标方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，由投标方承担相应责任。

7. 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，并且在应答文件中需写出具体的工具介绍。

8. 保密要求

- 投标方应与委托方签订保密协议。如果参与测试的人员在规定的保密期内发生失泄密行为，投标方应承担全部责任。
- 投标方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。保密责任最终以正式签署的保密协议为准。
- 在未经采购人书面同意的情况下，投标方不得将本项目、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。否则，投标方必须承担因此给采购人造成的一切经济损失，采购人保留追究法律责任的权力。投标方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。

9. 进度要求

系统上线后六个月内完成。