

## 第三包：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. 监理服务内容及要求

在监理服务范围内，依据国家有关信息系统的法律、法规、技术规程、规范、标准以及工程建设文件，监理单位承担全部工作的监理服务，按照《信息化工程监理规范》(GB/T 19668-2014)总则及各分册的要求，对各系统的质量、进度、投资、风险进行全方位、全过程控制，进行项目的合同管理、变更管理、配置管理、文档管理、人员管理、信息管理以及安全文明实施的监理，负责系统建设过程中的组织协调等工作，使项目建设按既定目标顺利进行。

#### 一) 监理服务内容

对本项目实施全过程监理,包括硬件系统(包括网络、服务器、存储、计算机、监控系统等项目涉及的所有设备)及软件系统(建设内容中所涉及的所有软件系统);协助建设方与承建方更详细完整地定义业务需求,控制成本增加,避免实施过程中不断的项目变更协助建设方与承建方更详细完整地定义业务需求,控制成本增加,避免实施过程中不断的项目变更。因项目需求发生变化;确保项目的整体解决方案具备先进性、经济实用性、成熟性、可靠性、安全性、可管理性和可扩展性;确保项目实施的软硬件设备能达到业务需求,且趋于智能化和先进性。因项目需求发生变化,而增加的其他子项系统,也列入监理范围内。建设工程项目施工阶段的质量、进度、费用控制管理和安全、合同、信息等方面协调管理服务。

#### 二) 监理服务范围

负责对项目的全部建设内容,包括建设方案深化设计、建设实施、技术培训、试运行、系统验收等进行全过程监理。

#### 三) 监理服务周期

自监理合同签订之日起至项目通过竣工验收止。

#### 四) 监理服务要求

按照建设目标和要求,遵循《信息系统工程监理规范》,依据项目建设合同和用户需求,采用先进、科学、合理的适合本项目特点的项目管理技巧和手段,对项目的各个层面进行全方位的管理、控制和协调。对项目的设备和系统的购置、安装调试、基础数据准备、技术培训等方面质量、进度、投资和信息安全等进行全面控制;对项目建设合同的执行、项目建设文件资料等进行管理,从而使本项目“按期、保质、高效、节约”的完成。

#### 五) 监理服务内容

##### 1、项目组织及技术总体方案的把关

- (1) 审核和确认承建单位的总体设计方案;
- (2) 审核和确认项目建设过程中的各种关键技术方案;
- (3) 审核和确认承建单位的组织和实施方案、投标人提交的《项目计划》;
- (4) 审核和确认承建单位的项目质量保证计划、质量控制体系(含质量控制的关键性节点);
- (5) 审核和确认承建单位的项目进度计划和进度控制节点;

##### 2、项目质量控制

###### (1) 系统集成质量的控制

- 1) 系统集成方案的审核和确认;
- 2) 审核关键设备、系统软件选型方案,协助系统集成商和建设方进行选型;
- 3) 对采购的硬件设备的质量进行检验、测试和验收;
- 4) 对设备安装、系统软件的安装调试进行验收;
- 5) 对系统集成进行总体验收。

###### (2) 应用软件开发质量的控制

- 1) 应用软件开发阶段性计划的审核和确认;
- 2) 在对项目建设详细了解的基础上,协助项目承建单位和业主单位,对各个分系统、子系统应用软件的详细需求分析、详细设计、编码测试、系统安装调试、系统试运行进行把关;
- 3) 对承建单位的开发质量进行审核;

4) 对源代码、开发文件进行移交验收。

(3) 软件应用培训的质量控制

1) 审核确认承建单位的培训计划；

2) 监督承建单位实施其培训计划，并征求用户的反馈意见；

3) 审核确认承建单位的培训总结报告。

3、项目进度控制

(1) 审核承建单位的进度分解计划，确认分解计划可以保证总体计划目标；

(2) 对项目实施进度进行实时跟踪，并要求承建单位对进度计划进行动态调整，以确保项目的阶段和总体进度目标的实现；

(3) 当工期目标严重偏离时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

4、项目投资控制

(1) 通过对项目实施中的方案及设计的优化，确保投资控制在合理、性价比高的范围内；

(2) 协助采购人做好项目支付预算的现金流量表，将付款进度与项目质量与形象进度结合起来。

5、项目合同管理

(1) 跟踪检查合同的执行情况，确保承建单位按时履约；

(2) 对合同工期的延误和延期进行审核确认；

(3) 对合同变更、索赔等事宜进行审核确认；

(4) 根据合同约定，审核承建单位提交的支付申请，签发付款凭证。

6、信息管理/项目文档管理

(1) 做好监理日记及项目大事记；

(2) 做好合同批复等各类往来文件的批复和存档；

(3) 做好项目协调会、技术专题会的会议纪要；

(4) 管理好实施期间的各类技术文档；

(5) 项目周报；

(6) 监理建议书；

- (7) 监理通知；
- (8) 各种会议纪要；
- (9) 阶段性项目总结；
- (10) 各承建方提交的技术文档。

7、经业主委托，负责协调本项目所涉及的各承建单位之间的工作关系，并协调解决项目建设过程中的各类纠纷。

监理方应该通过必要的会议制度来实施协调工作，主要包括：

- (1) 现场会；
- (2) 监理交底会；
- (3) 周例会；
- (4) 监理协调会；
- (5) 专题讨论会；
- (6) 专家论证会；
- (7) 阶段工作总结会；
- (8) 问题通报会；
- (9) 阶段及最终验收会。

## 8、项目安全的管理

- (1) 负责项目建设过程中所涉及的政府机密数据和资料的保护，保证不被非授权使用；
- (2) 负责项目建设施工过程中安全控制，确保不出现安全事故。

## 9、项目知识产权的管理

- (1) 负责项目建设过程中所产生成果的知识产权保护，保证不被非授权使用；
- (2) 负责项目建设过程中涉及知识产权的产品和系统的使用审核，保证业主方不在本项目建设中出现违反知识产权的行为。

## 10、项目的协调和组织

- (1) 确定承建单位的工作范围和职责；建立畅通的沟通平台和沟通渠道，采取有效措施使项目信息在有关各方之间保持顺畅流通，积极协调项目各方之间的关系，推动项目实施过程中问题的解决。

(2) 接受委托，负责协调项目所涉及的各单位之间的工作关系，并协调解决项目建设过程中的各类纠纷。监督各方履行职责，协调各方的工作关系；

(3) 监理方应通过必要的会议制度来实施协调工作，主要包括项目例会、专题讨论会、专家评审会、问题通报会、监理协调会、监理交底会阶段工作总结会、阶段以及最终验收会和参与采购单位组织的有关会议等。

## **2. 监理实施要求**

监理方不得将监理工程进行分包或转包，否则招标方有权终止合同，并由监理方承担由此造成的一切损失。

投标人应建立本项目实施过程的组织方式、日常工作管理方式、日常计划管理方式及质量保障控制手段。

1、本项目实行总监理工程师负责制。拟派总监理工程师和总监理工程师代表具有信息系统监理师和信息系统项目管理师证书，以及5年以上从事信息系统工程监理工作的经历。

2、组建工程监理机构。监理机构由总监理工程师、总监代表和专业监理工程师组成，人数在5人以上。所有人员均应具备信息系统监理师资格证书，监理队伍人员配置应专业齐全。监理人员应能常驻现场、吃苦耐劳、认真负责、秉公办事、廉洁自律。

3、检测工具：监理组必须配备符合项目专业特点的检测仪器和设备，满足项目检测需要。

4、服务方式：要求中标的投标人以驻施工现场监理为主要方式进行。

## **3. 监理服务准则**

1、维护国家和采购人的荣誉和利益，按照“守法、诚信、公正、科学”的准则执业。

2、遵守国家的法律和政府的有关条例、规定和办法等。

3、执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责。

4、坚持科学的态度和实事求是的原则。

- 5、认真履行项目建设监理合同所承诺的义务和承担约定的责任。
- 6、坚持公正的立场，公平地处理有关各方的争议。
- 7、不收受被监理单位的任何礼金。
- 8、不泄漏所监理的项目需保密的事项。
- 9、不泄漏所监理项目各方认为需要保密的事项。

## 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、软件测试师、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。需完成工作包括但不限于：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 and 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](http://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。

## 第六包：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，商用密码应用安全性评估工作的开展是保障本项目能最终验收的必要环节以及今后该信息系统商密改造的依据。

### 2. 工作内容

本次评估项目的开展，目的是检验应用系统在密码应用方面是否符合国家相关规范和要求，密码技术、密码产品、密码管理等方面是否符合相关标准。

评估对象可能涉及信息系统部署相关的机房、网络环境、服务器、数据库、应用系统及安全管理等方面。

### 3. 服务依据

- ✧ 《中华人民共和国网络安全法》
- ✧ 《中华人民共和国密码法》
- ✧ 《关键信息基础设施保护条例》（征求意见稿）
- ✧ 《商用密码管理条例》
- ✧ GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》
- ✧ GM/T 0115-2021 《信息系统密码应用测评要求》
- ✧ GM/T 0116-2021 《信息系统密码应用测评过程指南》



#### 4. 测评指标及内容

《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中对不同等级密码系统的安全功能和措施作出具体要求，密码安全测评要根据信息系统的等级从中选取相应等级的商用密码应用安全性评估工作指标，并根据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》的相应等级要求，对本项目涉及的本次建设信息系统根据定级情况实施商用密码应用安全性评估工作，以下为等保三级系统的商用密码应用安全性要求：

测评单元			测评指标	应用要求
技术要求	物理和环境安全	身份鉴别	8.1 a) 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；	宜
		电子门禁记录数据存储完整性	8.1 b) 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；	宜
		视频监控记录数据存储完整性	8.1 c) 宜采用密码技术保证视频监控音像记录数据的存储完整性。	宜
	网络和通信安全	身份鉴别	8.2 a) 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；	应
		通信数据完整性	8.2 b) 宜采用密码技术保证通信过程中数据的完整性；	宜
		通信过程中重要数据的机密性	8.2 c) 应采用密码技术保证通信过程中重要数据的机密性；	应
		网络边界访问控制信息的完整性	8.2 d) 宜采用密码技术保证网络边界访问控制信息的完整性；	宜
		安全接入认证	8.2 e) 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。	可
	设备和计算安全	身份鉴别	8.3 a) 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；	应
		远程管理通道安全	8.3 b) 远程管理设备时，应采用密码技术建立安全的信息传输通道；	应
		系统资源访问	8.3 c) 宜采用密码技术保证系统资源访问	宜

		控制信息完整性	控制信息的完整性；	
		重要信息资源安全标记完整性	8.3 d) 宜采用密码技术保证设备中的重要信息资源安全标记的完整性；	宜
		日志记录完整性	8.3 e) 宜采用密码技术保证日志记录的完整性；	宜
		重要可执行程序完整性、重要可执行程序来源真实性	8.3 f) 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。	宜
	应用和数据安全	身份鉴别	8.4 a) 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；	应
		访问控制信息完整性	8.4 b) 宜采用密码技术保证信息系统应用的访问控制信息的完整性；	宜
		重要信息资源安全标记完整性	8.4 c) 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；	宜
		重要数据传输机密性	8.4 d) 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；	应
		重要数据存储机密性	8.4 e) 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；	应
		重要数据传输完整性	8.4 f) 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；	宜
		重要数据存储完整性	8.4 g) 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；	宜
		不可否认性	8.4 h) 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	宜
管理要求	管理制度	具备密码应用安全管理制度	8.5 a) 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；	应
		密钥管理规则	8.5 b) 应根据密码应用方案建立相应密钥管理规则；	应
		建立操作规程	8.5 c) 应对管理人员或操作人员执行的日常管理操作建立操作规程；	应
		定期修订安全管理制度	8.5 d) 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，	应

			对存在不足或需要改进之处进行修订；	
		明确管理制度发布流程	8.5 e) 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；	应
		制度执行过程记录留存	8.5 f) 应具有密码应用操作规程的相关执行记录并妥善保存。	应
	人员管理	了解并遵守密码相关法律法规和密码管理制度	8.6 a) 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；	应
		建立密码应用岗位责任制度	8.6 b) 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限： 1) 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2) 对关键岗位建立多人共管机制； 3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 4) 相关设备与系统的管理和使用账号不得多人共用。	应
		建立上岗人员培训制度	8.6 c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；	应
		定期进行安全岗位人员考核	8.6 d) 应定期对密码应用安全岗位人员进行考核；	应
		建立关键岗位人员保密制度和调离制度	8.6 e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。	应
	建设运行	制定密码应用方案	8.7 a) 应依据密码相关标准和密码应用需求，制定密码应用方案；	应
		制定密钥安全管理策略	8.7 b) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录 A；	应
		制定实施方案	8.7 c) 应按照应用方案实施建设；	应
		投入运行前进	8.7 d) 投入运行前应进行密码应用安全性评	应

		行密码应用安全性评估	估，评估通过后系统方可正式运行；	
		定期开展密码应用安全性评估及攻防对抗演习	8.7 e) 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。	应
	应急处置	应急策略	8.8 a) 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；	应
		事件处置	8.8 b) 事件发生后，应及时向信息系统主管部门进行报告；	应
		向有关主管部门上报处置情况	8.8 c) 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。	应
	测评指标合计		41 项	

## 5. 测评方法

商用密码应用安全性评估工作（以下简称密评）的主要方式有：访谈、检查和测试。

**访谈：**访谈是指测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据表明信息系统安全保护措施是否落实的一种方法。在访谈的范围上，应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

**检查：**检查是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在检查范围上，应基本覆盖所有的对象种类（设备、文档、机制等），数量上可以抽样。

**测试：**测试是指测评人员通过对测评对象按照预定的方法/工具使其产生特定的响应等活动，查看、分析响应输出结果，获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在测试范围上，应基本覆盖不同类型的机制，在数量上可以抽样。

测试过程需采用密码专用分析工具对密码算法实现等内容进行深度测试。

## 6. 项目实施内容

本次密码应用安全性测评实施，需通过测评准备、方案编制、现场测评、分析与报告编制等几个阶段开展：

（1）测评准备：主要任务是掌握被测系统的详细情况，准备测评工具，为编制测评方案做好准备。

（2）方案编制：方案编制活动的目标是整理测评准备活动中获取的信息系统相关资料，为现场测评活动提供最基本的文档和指导方案。方案编制活动包括测评对象确定、测评指标确定、测评检查点确定、测评内容确定及测评方案编制五项主要任务。

（3）现场测评：依据测评方案将测评方案和测评工具等具体落实到现场测评活动中，实施现场测评和结果记录。

（4）分析与报告编制：根据单元测评、整体测评结果，分析信息系统在密码应用层面存在的安全问题，以及问题造成的影响、问题的严重程度，给出安全问题处置建议。根据密码应用安全性评估报告模板，出具符合国家密码管理部门要求的评估报告，并在报告中明确测评对象、测评指标、测评内容、测评结果、问题和整改建议、测评结论等内容。

（5）信息系统商用密码应用改造方案支撑工作：根据本项目的密评结果即整改建议，协助投标人对本项目涉及的信息系统制定完善可行的商用密码应用安全性改造方案并通过专家评审，作为该系统今后商用密码应用安全性改造工作的实施依据。

## 7. 进度要求

信息系统上线后 6 个月内完成（不含项目整改时间）。

## 8. 产出成果

本次针对本项目涉及的信息系统的密码应用安全性评估，本项目交付物包括但不限于：

《商用密码应用安全性评估实施方案》，要求提交纸质版（3 份）和电子版。

《商用密码应用安全整改建议》，要求提交纸质版（3 份）和电子版。

《商用密码应用安全性评估报告》，每个信息系统评估报告要提交纸质版（3 份）。

《商用密码应用安全性改造方案》，并通过密码局的专家评审。需要提交纸质版（3 份）。

## **9. 验收要求**

投标人递交正式《商用密码应用安全性评估报告》和《整改建议书》后，招标人视为验收通过。

## **10. 进度要求**

系统上线后六个月内完成。