#  采购需求

一**、采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 包号 | 包名 | 单位 | 采购限价（元） |
| 1 | 2022年网络安全等级保护测评服务 | 项 | 310000.00 |

1. **技术参数**

**1、项目服务范围**

委托获得公安部认证资质的测评机构，对招标人的2个三级（S3A3G3）信息系统和3个二级（S2A2G2）信息系统安全保护状况进行分等级测试评估---等级测评，按系统出具《网络安全等级保护等级测评报告》，并结合招标人单位的实际情况，出具《安全建设整改设计方案》。

|  |  |  |
| --- | --- | --- |
| **序号** | **信息系统名称** | **安全保护等级** |
| 1 | HIS系统 | 第三级 S3A3G3 |
| 2 | 医院信息集成平台 | 第三级 S3A3G3 |
| 3 | 门户网站 | 第二级 S2A2G2 |
| 4 | LIS检验信息管理系统 | 第二级 S2A2G2 |
| 5 | 全院级PACS影像信息系统 | 第二级 S2A2G2 |

## 2、项目服务内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **服务期限** | **服务内容** | **服务范围** |
| 1 | 网络安全等级保护测评服务 | 自合同生效且收到招标人开工令之日起60日内完成 | 依据《网络安全等级保护基本要求》等有关管理规范和技术标准，对等级保护对象的安全物理环境、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层面的安全测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，并提出整改建议。 | 本项目中需开展等保测评的2个三级（S3A3G3）信息系统和3个二级（S2A2G2）信息系统 |
| 2 | 安全建设整改方案设计服务 | 自合同生效且收到招标人开工令之日起60日内完成 | 在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》(公信安[2009]1429号)的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。 | 本项目中需开展等保测评的2个三级（S3A3G3）信息系统和3个二级（S2A2G2）信息系统 |
| 3 | 售后服务 | 网络安全咨询服务 | 1 | 年 | 自项目验收之日起，提供1年期的网络安全等级保护咨询服务。 | 海南医学院第一附属医院 |

## 3、项目服务要求

### 3.1网络安全等级保护测评服务

投标人自合同生效且收到招标人开工令之日起60日内，完成网络安全等级保护测评服务。投标人对招标人的2个三级（S3A3G3）信息系统和3个二级（S2A2G2）信息系统完成等级保护对象要素进行确认、分析和梳理，提出详细的等级测评方案。对等级保护对象的整体保护状况和等级保护组件，逐一进行网络安全等级保护等级测评，等级测评的内容包括以下内容: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、安全运维管理十个层面的测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，针对等级保护对象安全建设提出整改建议。

**3.1.1测评实施过程**

投标人在测评过程中，按照《信息安全技术 网络安全等级保护测评过程指南》等标准开展测评实施工作，等级测评过程分为四个基本测评活动:测评准备活动、方案编制活动、现场测评活动、报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。 测评双方之间的沟通与洽谈应贯穿整个等保测评过程。

**3.1.1.1测评准备活动**

测评准备活动的目标是顺利启动测评项目,收集定级对象相关资料,准备测评所需资料,为编制测评方案打下良好的基础。

测评准备工作应包括工作启动、信息收集和分析、工具和表单准备。

详细要求见下表：

|  |  |  |
| --- | --- | --- |
| **项目内容** | **工作内容** | **成果输出** |
| 项目启动 | 1.组建测评项目组 | 向测评委托单位提交《项目计划书》、《提供资料清单》 |
| 2.编制《项目计划书》 |
| 3.确定测评委托单位应提供的资料 |
| 信息收集分析 | 1.整理调查表单 | 《等级保护对象调查表》 |
| 2.发放调查表单给测评委托单位 |
| 3.协助测评委托单位填写调查表 |
| 4.收回调查结果 |
| 5.分析调查结查 |
| 工具和表单准备 | 1.调试测评工具 | 确定测评工具（测评工具清单）《现场测评授权书》打印各类表单:风险告知书、文档交接单、会议记录表单、会议签到表单 |
| 2.模拟被测定级对象架构，熟悉被测定级对象  |
| 3.准备和打印各类表单  |

**3.1.1.2方案编制活动**

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。

方案编制活动应包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

|  |  |  |
| --- | --- | --- |
| **工作内容** | **工作详细任务** | **输出成果** |
| 一、测评对象确认 | 分析并确定被测定级对象识别并描述被测定级对象的整体结构识别并描述被测定级对象的边界识别并描述被测定级对象的网络区域识别并描述被测定级对象的主要设备确定测评对象描述测评对象 | 《测评方案》的测评对象部分 |
| 二、测评指标确定 | 确定被测定级对象业务信息和系统服务安全保护等级 | 《测评方案》的测评指标部分 |
| 根据被测定级对象的A 类、S类及G 类基本安全要求的组合情况,从GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标 |
| 根据测评委托单位及被测定级对象业务自身需求, 确定特殊测评指标。 |
| 根据测评委托单位及被测定级对象业务自身需求, 确定特殊测评指标。 |
| 对确定基本测评指标和特殊测评指标进行描述,并分析给出指标不适用的原因 |
| 三、测评内 容确定 | 确定每个测评对象对应的每个测评指标的测评方法 | 《测评方案》的单项测评实施部分 |
| 确定实施测评的单项测评内容 |
| 四、工具测试点确定 | 确定工具测试环境 确定工具测试工具 确定工具测试的测评对象 选择测试路径 确定测试工具的接入点 本次项目测评需要使用到如下工具: 漏洞扫描工具; Windows 主机安全配置检查工具; Linux 主机配置检查工具; 网络及安全设备配置检查工具; 病毒检查工具; 木马检查工具;网站恶意代码检查工具;在线检查工具(网站安全检查工具);终端安全检查工具;口令破解工具;渗透测试工具;SQL 注入验证检查工具; 在线数据库安全检查工具。  | 《测评方案》的的工具测试方法及内容部分 |
| 五、测评指导书开发 | 确定单个测评对象，内容包含测评对象的名称、位置信息、用途、管理人员等信息 | 测评指导书、测评结果记录表格 |
| 确定单项测评实施活动,包括测评项、测评方法、操作步骤和预期结果等四部分  |
| 确定单项测评、整体测评表述形式 |
| 根据测评指导书,形成测评结果记录表格  |
| 六、测评方案编制 | 明确项目整体情况和测评活动依据 | 向测评委托单位提交经过评审和确认的《测评方案》、《风险规避实施方案》 |
| 根据测评协议书和被测定级对象情况,估算现场测 评工作量  |
| 根据测评项目组成员安排,编制工作安排情况  |
| 根据以往测评经验以及被测定级对象规模,编制具体测评计划,包括现场工作人员的分工和时间安排  |
| 汇总上述内容及方案编制活动的其他任务获取的 |
| 内容形成测评方案文稿  |
| 评审和提交测评方案  |
| 根据测评方案制定风险规避实施方案 |

**3.1.1.3现场测评活动**

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展 打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作主要取得报告编制活动所需的、足够的证据和资料。

 现场测评活动应包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

|  |  |  |
| --- | --- | --- |
| **工作内容** | **工作详细任务** | **输出** |
| 1.现场测评准备 | 测评委托单位对风险告知书签字确认 | 会议记录，风险告知书，测评方案和现场测评工作计划，现场测评授权书 |
| 测评委托单位协助测评机构签署现场测评授权书 |
| 召开现场测评首次会  |
| 双方确认测评计划和测评方案 |
| 双方确认配合人员、测评环境等各种现场测评需要的资源 |
| 2.现场测评和结果记录 | 确认测评对象的关键数据已经进行了备份 | 《各类测评结果记录/测评证据 和证据源记录/文档交接/规划 记录单》 访谈结果: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、安全运维管理安全测 评的测评结果记录或录音 ; 文档审查结果: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、安全运维管理测评的测评结果记录;配置核查结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格工具测试结果: 安全物理环 境、安全通信网络、安全区域 边界、安全计算环境、安全管理中心测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件实地察看结果: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、安全运维管理测评结果记录测评结果确认:现场核查中发现的问题汇总、测评证据和证据源记录、测评委托单位的书面认可文件 |
| 确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状况 |
| 根据测评指导书实施现场测评，获取相关证据和信息 |
| 测评结束后，双方确认测评工作是否对测评对象造成不良影响,测评对象及系统是否工作正常  |
| 3.结果确认和资料归还 | 汇总测评记录，对漏掉和需要进一步验证的内容实施补充测评 |
| 召开现场测评结束会，测评双方对测评过程中得到的证据源记录进行确认 |
| 测评人员归还借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认 |

**3.1.1.4报告编制活动**

 在现场测评工作结束后，应对现场测评获得的测评结果(或称测评证据)进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估, 经过整体测评后,有的单项测评结果可能会有所变化, 需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。报告编制活动应包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成及测评报告编制七项主要任务。

详细要求见下表：

|  |  |  |
| --- | --- | --- |
| **工作内容** | **工作详细任务** | **工作依据（模版）** |
| 1.单项测评结果判定 | 分析测评项所对抗威胁的存在情况 | 测评报告的等级测评结果记录部分 |
| 分析单项测评项的测评证据,并与要求内容的预期测评结果相比较,给出单项测评 结果和符合程度得分  |
| 综合判定单项测评项的测评结果 |
| 2.单元测评结果判定 | 汇总不同测评对象对应测评指标的单项测评结果情况 | 测评报告的单元测评小结部分 |
| 判定每个测评对象的单元测评结果 |
| 3.整体测评 | 分析不符合和部分符合的测评项与其他测评项(包括安全控制点、安全控制点间、区域间)之间的关联关系及对结果的影响情况 | 测评报告的整体测评部分  |
| 根据整体测评分析情况,修正单项测评结果符合程度得分和问题严重程度值  |
| 4.系统安全 保障评估  | 根据整体测评结果,计算修正后的每个测评对象的单项测评结果和符合程度得分  | 测评报告的系统安全保障评估部分 |
| 根据各对象的单项符合程度得分,计算安全控制点得分  |
| 根据安全控制点得分,计算安全层面得分 |
| 根据安全控制点得分和安全层面得分,总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况  |
| 5.安全问题 风险分析  | 针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题,结合关联测评 对象和威胁,分析可能对定级对象、单位、社会及国家造成的安全危害  | 测评报告的安全问题风险分析部分 |
| 结合安全问题所影响业务的重要程度、 相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危 害(损失)结果  |
| 根据最大安全危害严重程度进一步确定定级对象面临的风险等级,结果为“高”“中”或“低”  |
| 6.等级测评结论形成 | 统计再次汇总后的单项测评结果为部分符合和不符合项的项数 | 等级测评报告的等级测评结论部分 |
| 计算定级对象综合得分，形成等级测评结论，形成等级测评结论 |
| 7.测评报告编制 | 概述测评项目情况，整理前面几项任务的输出/产品  | 经过评审和确认的被测定级对象等级测评报告 |
| 针对被测定级对象存在的安全隐患，提出处置建议 |
| 根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息,对测评报告进行评审  |
| 评审通过后,由项目负责人签字确认并提交给测评委托单位  |

**3.1.1.5 测评实施活动文档**

 测评机构在上述各阶段活动的测评实施服务过程中，根据服务规范和测评委托单位要求，提供系统、完整、清晰的服务日常报告。

 提供的服务文档应至少但不限于如下文档:

**测评准备活动阶段:**

 《项目计划书》;

 《等级保护对象调查表》;

 《会议记录表》;

**方案编制活动阶段:**

 《网络安全等级保护测评方案》;

 《测评指导书》;

《风险规避实施方案》;

**现场测评活动阶段:**

《现场测评授权书》;

《文档交接单》;

《会议记录》;

**报告编制活动阶段:**

 按系统提交《网络安全等级保护等级测评报告》，并针对该信息系统提出安全整改建议。

### 3.2 安全建设整改方案设计服务

 投标人自合同生效且收到招标人开工令之日起60日内，投标人在完成网络安全等级保护等级测评后，根据本项目相关网络安全等级保护等级测评报告，针对等级测评过程发现的问题，将依据网络安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》(公信安[2009]1429号)的规定，并结合本项目招标人单位的实际情况，出具《安全建设整改设计方案》。

### 3.3网络安全咨询服务

#### 3.3.1网络安全政策/标准咨询

随着国家网络安全等级保护的工作推进，网络安全等级保护政策、法律法规和标准体系也会相应的发布和更新，投标人应针对本项目设立网络安全等级保护咨询平台，自合同验收之日起，提供1年咨询服务，咨询内容包括但不限于网络安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

#### 3.3.2等级保护对象等级变更咨询

目前海南医学院第一附属医院的信息系统部分完成信息系统的定级备案工作。随着信息系统的不断建设和发展，可能会出现信息系统等级变更情况。在信息系统出现等级变更时，投标人需协助海南医学院第一附属医院对信息系统进行识别，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

定级阶段，投标人需根据等保相关主管部门和国家工信部的要求和指南，协助海南医学院第一附属医院完成定级对象确认、系统定级和定级备案工作。

#### 3.3.3等级保护自查咨询

按照等级保护相关政策要求，信息系统运营使用单位应定期对信息系统进行自查活动，在自查活动期间，投标人应提供海南医学院第一附属医院相应的咨询服务。

## 4、项目的实施要求

项目实施过程中，投标方应遵循国家标准、行业标准。

### 4.1项目实施要求

在项目实施中投标方必须做到：

1. 提供项目实施组织架构；
2. 提供详细的项目实施方案和计划进度说明书；
3. 投标人应定期向招标人汇报项目的实施进度，包括但不限于项目经理在项目期间每周至少来招标人现场1次进行工作汇报，且电话要保持7\*24小时通畅；
4. 为保障项目服务响应速度，投标人承诺项目实施期间及售后服务期内，提供本地化技术支持服务，对于招标人的电话咨询和常规服务请求在30分钟内予以答复，紧急服务请求在2小时内到达招标人现场；
5. 严格按照双方确定的计划进度保质保量完成工作；
6. 规范项目实施过程中的文档管理；
7. 项目实施中要引入风险管理、质量管理、成本管理；
8. 实施人员必须签署《保密协议》，按照《保密协议》的要求开展相关工作。

### 4.2实施团队要求

本项目实施团队成员名单及职责分工明确，项目期间在项目本地部署不少于10人的测评师团队，项目经理必须具有3年以上的等保测评服务项目管理经验，且每周到项目现场不少于一天；其中，本项目实施成员中，至少有2人具备等级保护高级测评师资格和有3人具备等级保护中级测评师资格，且属于投标人在册员工(以社保缴纳证明为认定依据)，实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《信息安全等级测评师证书》或中关村信息安全测评联盟颁发的《网络安全等级测评师证书》（以下统一简称为“测评师证书”），且在项目现场随身佩戴《测评师证书》备查。实施团队名单中所列人员的社保缴纳证明和《测评师证书》复印件需在投标文件中提供，并加盖公章。

### 4.3项目验收

投标方必须书面通知招标方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经招标方认定后方可执行。

### 4.4验收组织

成立由招标方、中标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

### 4.5验收标准

* 完成了本项目内所有的服务工作；
* 提交本项目内所有服务工作的服务成果；
* 提交项目实施阶段所有的过程文档。

## 5、项目工期

 投标人自合同生效且收到招标人开工令之日起60日内，完成网络安全等级保护测评服务并提交《网络安全等级保护等级测评报告》和《安全建设整改设计方案》。