采购需求

1、项目名称：**徐州市第一人民医院等保测评（2025年度）服务**

**2、项目目标**

2.1、委托具备资质的第三方信息安全等级测评机构（以下简称“测评机构”）对单位拟定级的信息系统进行网络安全等级保护测评，查找与分析现有系统的安全防护能力的不足，编制等级保护测评报告，并协助采购方完成测评报告的备案。

2.2、根据等级测评成果，由测评机构提出合理可行的安全整改建议，协助甲方进行安全管理与安全技术两方面的整改工作。

本次项目中待测评系统清单如下：

**三级系统（2个）： 智慧医疗信息系统、信息集成平台系统**

**3、项目具体内容**

3.1开展信息系统安全等级保护测评。根据《信息安全等级保护管理办法》等标准规范要求，对徐州市第一人民医院信息系统开展等级保护测评工作；具体测评内容包括但不限于：

（1）安全物理环境

测评内容主要包括：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、电磁防护等。

（2）安全通信网络

测评内容主要包括：网络架构、通信传输、可信验证等。

（3）安全区域边界

测评内容主要包括：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、可信验证等。

（4）安全计算环境

测评内容主要包括：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、数据保密性、数据完整性、数据备份恢复、剩余信息保护、个人信息保护等。

（5）安全管理中心

测评内容主要包括：系统管理、审计管理、安全管理、集中管控等。

（6）安全管理机构

测评内容主要包括：安全管理机构设置、人员配备及职责、安全授权和审批、安全沟通和合作、安全审核和检查等。

涉及信息安全工作领导小组、人员岗位设置、相关日常工作执行情况等。

（7）安全管理制度

测评内容主要包括：安全管理制度内容、制度的制定与发布、制度的评审和修订等。

涉及信息安全的总体方针、安全策略、管理制度、操作规程等。

（8）安全管理人员

测评内容主要包括：人员岗位管理、人员培训与考核、人员安全意识教育、外部人员访问管理等。

涉及安全相关人员，如安全主管、人事主管、运维主管、网络安全管理员、主机安全管理员、应用安全管理员、机房值班人员、资产管理人员、文档管理员等。

（9）安全建设管理

测评内容主要包括：安全设计管理、产品采购使用管理、自行软件开发管理、外包软件开发管理、安全工程实施管理、安全测试验收管理、安全系统交付管理、安全服务选择管理等。

涉及系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，以及产品采购、软件开发、工程管理与交付验收等相关流程与配套文件等。

（10）安全运维管理

测评内容主要包括：运行环境管理、资产管理、存储介质管理、设备管理、安全审计管理、入侵防范管理、网络安全管理、主机系统安全管理、用户授权管理、备份与恢复管理、恶意代码防范管理、安全事件处置管理、应急响应管理等。

涉及系统运维管理方面的流程、措施、制度、文档等。

项目正式启动后将向测评机构提供详细资产清单与网络拓扑结构图。

3.2从系统现状出发，依据《信息系统安全等级保护测评要求》等技术标准进行差距分析，明确甲方重要信息系统中存在的风险和相关脆弱点，并针对系统存在的主要问题提出安全建设、整改建议，制订《系统安全建设整改建议》。

3.3开展信息安全等级保护安全管理制度建设，提高信息系统安全管理水平。按照《信息安全等级保护管理办法》、《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，建立健全并落实符合相应等级要求的安全管理制度。

**4、网络安全保障服务**

4.1、等级保护要求

（1）测评完成之后，提供《系统信息安全等级保护测评报告》和《系统信息安全等级保护整改方案》（每个系统一份）。

（2）为业主提供次2信息安全技术培训。

（2）为业主提供次漏洞扫描、渗透测试服务。

4.2、安全检测与巡检服务

服务期内针对信息化建设提供1次全面的安全检测服务和并提供每年4次巡检服务。保障网络和信息系统处于安全状态，杜绝带病运行的情况。

4.3、安全应急保障服务

依据网络安全主管单位相关专项应急预案要求及信息系统等级保护国家标准，对网 络安全应急预案和各重要系统预案进行梳理和修订，并据此开展网络安全应急演练工作 ，完善网络安全事件应急响应与安全事件通报机制。提供安全事件应急响应服务，60分钟响应，2小时达到现场；应急演练开展每年1次。

4.4、重要资产监测服务

针对测评系统中重要资产进行7\*24小时事件精准及时发现，从海量的安全日志中精准及时发现真实重要的安全事件，实现安全事件早发现、早处理。

一般事件快速处置：工作时间现场响应，帮助我单位对网络内服务资产爆发的一般安全事件（如：病毒攻击、恶意攻击等）进行清除，帮助我单位快速恢复业务，消除或减轻影响，闭环事件。

重大事件应急响应：重大事件应急快速响应，帮助我单位对事件进行紧急遏制、分析事件的影响范围、针对事件发生原因进行溯源排查、提供对应的安全加固方案等。

**5、项目管理要求**

**5.1实施要求**

（1）为了保证本次测评项目的实施质量和工期，本项目采用项目经理负责制、供应商安排具备一定信息安全技术能力、项目管理能力与等级测评工作经验的人员担任项目经理。除项目经理外，项目组至少由6名等级测评师组成。

（2）项目进场实施前，供应商必须与采购人签订项目保密协议。现场实施过程中测评人员必须接受甲方管理。

（3）供应商制定合理的时间计划安排。（项目工期：15个日历日）

（4）本次项目实施过程主要分为准备阶段、方案编制阶段、现场测评阶段、分析与报告编制四个主要项目阶段，供应商在方案中明确各阶段双方的主要工作，各阶段双方须相互配合协调的内容。

（5）为保证实施期间的系统安全运行，供应商应在合同期限内提供相应的应急响应服务，供应商的响应文件中须对期间可能出现的系统典型安全事件的处理流程与应急处理方法做出详细说明。

（6）供应商应具备完善的项目质量管理体系，在项目实施过程中项目经理应全程负责项目实施过程的把控。

**5.2标准依据**

《信息安全技术 信息系统安全等级保护定级指南》 （GB/T 22240-2020）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

《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）

《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

本次信息系统等级测评服务项目的实施流程、技术方法必须严格执行国家相关标准规范。

**5.3测评技术与方法**

供应商以访谈、现场勘查、上机查看、工具测试等方式开展测评工作，所有获取测评证据的过程尽可能不影响信息系统的正常运行，对于可能产生的负面影响（如有）供应商需要在响应文件中做具体描述。因目前信息系统均为B/S架构，在测评过程中测评机构需重点对WEB应用业务进行安全测试。

**6、其他**

1、签定合同日期：自中标（成交）通知书发出之日起7个工作日内按时签约。

2、服务时间：测评任务自合同签定之日起30个工作日内完成。

3、付款方式：按照合同实施和合同要求验收，甲方获得测评报告28天内，甲方向乙方支付服务费用的100%。

评分细则

一、本次招标评标采用综合评分法，即在满足招标文件实质性要求前提下，按照招标文件中规定的评分标准和各项因素进行综合评审，以评标总得分最高的投标人作为第一中标候选人，次高的作为第二中标候选人，以此类推。

1. 评标委员会各成员独立对每个进入打分程序的有效投标人的技术和商务部分以打分的形式进行评审和评价，评委会成员所打投标人之间同项分值相差过大的，评委会成员应说明评审及打分理由。
2. 对评委的评分（除价格分外）进行统计汇总并算术平均，计算出每个投标人的得分，加上价格得分即为每个投标人的评标总得分（满分100分）。所有计算结果均四舍五入保留小数点后两位。
3. 如出现评标总得分最高的投标人有两个或两个以上的，以投标报价较低者优先作为第一中标候选人，如果投标报价也相同的，则以抽签方式确定中标候选人排序。

|  |  |  |  |
| --- | --- | --- | --- |
| **内容** | **满分** | **项目** | **评分标准** |
| 报价部分 | 10分 | 报价  （10分） | 采用低价优先法计算，即满足竞争性磋商文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。  其他供应商的价格分按照下列公式计算（小数点保留两位）：报价分＝（评标基准价/最终投标报价）×10分。 |
| 商  务  部  分 | 26分 | 项目业绩  （4分） | 投标人自2022年5月1日以来，承接过徐州市及省内三甲医院等级保护测评相关服务案例，每提供1份，得1分，最高得4分。**（提供完整的合同复印件加盖公章，时间以合同签订时间为准）** |
| 企业评价  （6分） | 投标人具有质量管理体系认证，信息安全服务资质认证证书CCRC（应急处理服务资质），信息安全管理体系认证证书，合规管理体系认证证书，通信网络安全服务能力风险评估一级评定证书，ITSS运维管理体系认证证书，每提供1个得1分，最高得6分。**（提供有效的证书复印件加盖公章）** |
| 项目经理资质  （6分） | 针对本项目委派的项目经理（等级保护高级测评师）具备：PMP项目经理资质、CIIPT资质、CISAW资质、CCSC网络安全能力认证、CCRC数据安全官证书、CISP证书每有一项得1分，最高得6分。**（提供项目经理有效的证书复印件加盖公章，并提供投标人为其缴纳的近3个月社保证明材料复印件加盖公章）** |
| 质量经理资质（4分） | 针对本项目委派的质量经理（等级保护中级测评师）具备：CIIPT资质、CISAW（风险管理专业级）资质、CCRC数据安全官证书、CISP证书每有一项得1分，最高得4分。**（提供项目经理有效的证书复印件加盖公章，并提供投标人为其缴纳的近3个月社保证明材料复印件加盖公章）** |
| 项目组成员资质  （6分） | 针对本项目委派的项目组成员每有一人为中级测评师的，且具备PMP项目经理证书、CISP证书、CISAW（应急服务专业级）资质、CIIP-A资质、数据安全管理证书（中级）、一级建造师机电工程，每提供一个得1分，最高得6分。**（提供项目组成员有效的证书复印件加盖公章，并提供投标人为其缴纳的近3个月社保证明材料复印件加盖公章，各专业人员不得兼任）** |
| 技  术  部  分 | 54分 | 等级保护测评方案 （18分） | 对投标文件中提供的等级保护测评方案进行评价：  1.内容针对性强、科学、可操作的得18-13分；  2.内容针对性较强、较科学、较可操作的得12-7分；  3.内容针对性不强、不科学、不可操作的得6-0分。 |
| 等级保护实施方案 （18分） | 对投标文件中提供的等级保护实施方案进行评价：  1.内容针对性强、科学、可操作的得18-13分；  2.内容针对性较强、较科学、较可操作的得12-7分；  3.内容针对性不强、不科学、不可操作的得6-0分。 |
| 安全事件应急响应及保密管控方案  （18分） | 对投标文件中提供的安全事件应急响应及保密管控方案进行评价：  1.内容针对性强、科学、可操作的得18-13分；  2.内容针对性较强、较科学、较可操作的得12-7分；  3.内容针对性不强、不科学、不可操作的得6-0分。 |
| 增值  服务 | 10分 | 服务承诺  （10分） | 免费提供为期一年的网络安全保障服务，对各投标人投标文件中提供的网络安全保障服务方案进行综合评价：  1.内容针对性强、科学、可操作的得10-7分；  2.内容针对性较强、较科学、较可操作的得6-4分；  3.内容针对性不强、不科学、不可操作的得3-0分。 |