**绍兴市越城区人民医院等级保护测评服务项目招标方案**

**一、招标项目名称及数量 招标编号：ZHY-20220021**

|  |  |  |  |
| --- | --- | --- | --- |
| **标项** | **标段名称及数量****（详见招标文件）** | **预算金额或上限价****（单位：人民币元）** | **投标保证金****（单位：人民币元）** |
| 01标 | 等级保护测评服务项目 | ￥130000.00元 | ￥0.00 |

**二、投标供应商的资格要求**

1.满足《中华人民共和国政府采购法》第二十二条规定；未被“信用中国”（www.creditchina.gov.cn)、中国政府采购网（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

2.落实政府采购政策需满足的资格要求：供应商为中小企业；

3.本项目的特定资格要求：（无)。

**三、项目简介**

**一、服务清单及要求**

项目建设背景和必要性

（一）建设背景

等级保护是国家关于信息安全的基本政策，《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），（以下简称27号文）明确要求我国信息安全保障工作实行等级保护制度，提出“抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。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联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）（以下简称66号文）、《浙江省安全等级保护管理办法》（省政府第223号令）（以下简称223号令）进一步强调了开展信息安全等级保护工作的重要意义，规定了实施信息安全等级保护制度的原则、内容、职责分工、基本要求和实施计划，部署了实施信息安全等级保护工作的操作办法， 27号文、66号文和223号令不但为各行业开展信息安全等级保护工作指明了方向，同时也为各行业如何根据自身特点做好信息安全等级保护工作提出了更高的要求。

（二）项目依据

投标供应商应依据国家等级保护相关标准开展工作，依据标准（包括但不限于）如下国家标准：

1、《中华人民共和国网络安全法》；

2、中华人民共和国计算机信息系统安全保护条例（国务院第147号令）；

3、GB/T22239-2019《网络安全技术 网络安全等级保护基本要求》；

4、GB/T22240-2020《信息安全技术 网络安全等级保护定级指南》；

5、GB/T28449-2019《网络安全技术 网络安全等级保护测评过程指南》；

6、GB/T28448-2019《网络安全技术 网络安全等级保护测评要求》。

（三）项目建设必要性

《网络安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。根据《网络安全等级保护测评要求》等技术标准；第三级信息系统应当每年至少进行一次等级测评。

（四）项目原则

本次安全保护等级保护测评实施方案设计与具体实施应满足以下原则：

（1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购人的行为，否则采购人有权追究投标供应商的责任。

（2）标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

1.规范性原则：投标供应商的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪 和控制。

2.可控性原则：测评服务的进度要跟上进度表的安排，保证采购人对于测评工作的可控性。

3.整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

4.最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

**三、项目建设内容**

（一）招标范围

依据《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）、《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）、《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66号）和《信息安全等级保护管理办法》（公通字〔2007〕43号）等相关文件及标准要求，对招标人的信息系统进行等级测评及备案。其中包含以下信息系统：

|  |  |  |
| --- | --- | --- |
| 序号 | 系统名称 | 测评等级 |
| 1 | 门户网站系统 | 二级 |
| 2 | 面向患者服务系统（互联网医院） | 三级 |

（二）服务内容

等级保护测评应全面分析应用系统的安全保护措施与等级保护相应级别之间的差距，进行合规性分析，为系统等级保护加固整改提供客观依据，测评的内容包括但不限于以下内容：

一是安全通用要求（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）。

安全物理环境测评主要关注机房在物理位置选择、物理访问控制、供电等方面的安全保护能力， 具体测评指标描述如下表所示。

|  |  |  |
| --- | --- | --- |
| 序号 | 测评单元 | 测评项描述 |
| 1 | 安全物理环境 | 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、电力供应、电磁防护 |
| 2 | 安全通信网络 | 网络架构、通信传输、可信验证 |
| 3 | 安全区域边界 | 边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计和可信验证 |
| 4 | 安全计算环境 | 涉及身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、通信完整性、通信保密性、数据备份恢复、剩余信息保护、个人信息保护 |
| 5 | 安全管理中心 | 系统管理、审计管理、安全管理、集中管控 |
| 6 | 安全管理制度 | 安全策略、理制度体系、制定与发布、评审和修订 |
| 7 | 安全管理机构 | 岗位设置、人员配备、授权和审批、沟通与合作、审核与检查 |
| 8 | 安全管理人员 | 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 |
| 9 | 安全建设管理 | 系统定级、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、安全服务商选择 |
| 10 | 安全运维管理 | 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 |

二是根据各个系统的具体情况涉及到的各类扩展项。

（三）测评方法

测评方法必须符合 GB/T 28448-2019 信息系统安全等级保护测评要求，满足国家等级保护备案相关标准规范，在开展等级测评工作时，从管理和技术两个层面，通过多种方法来采集测评证据，以确定被测系统与基本要求之间的符合性。采集测评证据的方式分为“人员访谈”、“文件审核”、“现场观察”、“技术测试”等手段。

人员访谈：测评人员与被测单位信息技术人员进行面谈，测评人员可以了解其职责范围、工作陈述、基本安全意识、对安全管理获知的程度等信息。

文件检查：测评人员对被测单位与信息安全管理活动相关的所有文件进行审查，包括安全方针和 目标、程序文件、作业指导文件和记录文件等。

现场观察：测评人员通过到现场参观，观察并获取关于被测系统现场的物理环境、信息系统的安全操作和各类安全管理活动的第一手资料。

技术测试：测评人员通过对测评对象采用各种技术手段，获得被测系统在技术性控制的效力及符合性方面的证据。这些技术性措施包括：自动化的扫描工具、网络拓扑结构分析、本地主机审查、渗透测试等。

本次等级保护测评实施过程中所使用到的各种工具软件由供应商推荐，经采购人确认后由供应商提供并在测评中使用。供应商应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。等级保护测评应有详细的实施方案和严格的操作步骤，采取的措施应是经过测试、稳定可靠的。

安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由供应商推荐，经采购人确认后由供应商提供并在测评中使用。

安全测评需要的运行环境（如场地、网络环境等）由采购人提供，供应商应详细描述需要的运行 环境的具体要求。

（四）安全等级测评报告等要求

1.投标供应商应对采购人的信息系统进行等级保护测评，形成相应的测评报告；

2.投标供应商在测评后出具符合公安主管部门要求的系统安全保护等级测评报告；

3.对上述系统不符合网络安全等级保护有关管理规范和技术标准的，投标供应商出具可行的整改方案，并为采购人提供整改咨询服务；

4.投标供应商协助采购人完成信息系统安全保护等级测评的相关备案手续。

**★5.投标人必须获得为有效期内的经公安部第三研究所（国家认证认可委员会批准的认证机构）认证发放的《网络安全等级测评与检测评估机构服务认证证书》（技术文件中提供相关证明并加盖投标人公章）。**

**四、服务要求**

（一）本次等级保护测评的招标要求

1.投标供应商应提交本次等级保护测评的整体实施方案，包括项目概述、等保测评方案、项目实施方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交和验收标准等。

2.投标供应商应提交测评人员的组成、资质及各自职责的划分。投标供应商应配置有经验的测评人员进行本次等级保护测评工作。供应商实施骨干技术人员至少包含1名高级测评师。

3.本次等级保护测评实施过程中所使用到的各种工具软件由投标供应商推荐，经采购人确认后由投标供应商提供并在测评中使用。在投标文件中应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。

4.安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工作站等）和操作系统软件等由投标供应商推荐，经采购人确认后由投标供应商提供并在测评中使用。

5.安全测评需要的运行环境（如场地、网络环境等）由采购人提供，投标供应商应详细描述需要的运行环境的具体要求。

（二）本次等级保护测评实施要求

1.实施方应保证投标项目在本年度内完成测评工作；

2.实施方应根据采购方工作需求、进度要求、实际情况进一步完善《信息系统整体测评实施方案》，对项目目标、工作任务、阶段性工作、项目组织机构、职责分工、项目进度、质量控制等内容进行详细的说明，并通过采购方审核，以确保项目实施按时保质的完成；

3.实施方在项目实施过程中应服从采购方的统一领导和协调，采购方有权裁决实施方的责任范围，实施方必须执行，在采购方限定的时间内解决问题。如果实施方不能按时完成测评内容，采购方有权中止项目、索赔或拒付款项；

4.实施过程中形成的阶段性成果文件须指定相关责任人，明确相关职责；

5.在整改过程中，如需现场服务，实施方技术人员应赶到现场协助处理；

6.项目验收完成后，要求提供为期一年的技术咨询服务，以保证项目正常运行。

（三）本次等级保护测评保密要求

1.投标人必须和招标人签订保密协议，投标人必须要与参加此次测评项目的所有项目组成员签订保密协议，在合同签定时一并提供给招标人。

2.投标人具体测评工作和等级保护测评报告的编写，必须在招标人的指定地点进行。对于测评中的重要资料和结果，在测评期间和测评结束后，投标人不得带离该地点。

3.投标人对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论投标人中标与否，其对上述内容的保密责任将长期存在。

（四）项目服务承诺

1.投标供应商应满足采购人提出的标准性、规范性、可控性、整体性、最小影响性及保密性原则，做到守时、保质。

2.保密性要求：投标供应商必须和采购人签订保密协议和非侵害性协议，投标供应商必须要与参加此次测评项目的所有项目组成员签订保密协议和非侵害性协议，在合同签定时一并提供给采购人。

3.投标供应商具体测评工作和等级保护测评报告的编写，必须在采购人的指定地点进行。对于测评中的重要资料和结果，在测评期间和测评结束后，投标供应商不得带离该地点。

4.投标供应商对本规范书中的内容及在应标过程中接触的设备信息、数据资料等负有保密责任，不得泄露给任何第三方。无论投标供应商中标与否，其对上述内容的保密责任将长期存在。

5.等级保护测评的品质保证：投标供应商应承诺指派工作经验丰富、技术实力雄厚的安全顾问，结合技术领先、结论可靠的测评工具为客户作全面等级保护测评。承诺测评过程按照国家标准进行， 并保证对客户的资料严格保密。

（五）其它服务需求

1.测评结束后，针对每个测评的系统提出可行的整改方案，出具一份整改建议书，并提供整改咨询，并配合采购人做好整改工作的服务。

2.提供安全渗透测试服务:针对三级系统采用完全模拟入侵者可能采用的攻击技术和漏洞发现技术，利用专家经验对用户系统进行非破坏性质的模拟攻击，发现系统的最脆弱的环节和弱点等安全问题，为进一步加固信息系统提供了依据，并出具渗透测试报告。

3.在开展等级测评过程中，会发现信息系统存在的问题，需由测评服务单位出具《信息系统安全整改建议》并指导用户单位、系统开发商、集成商、设备厂商、安全服务商等进行系统安全整改加固工作。

4.结合国家、省、市有关要求，完成对采购人的系统测评，出具包括且不仅仅包括以下成果：符合绍兴市公安局要求的《等级保护测评报告》和《等级保护整改建议书》，测评工作结束后，协助招标方完成系统的备案工作。

**五、付款方式**

合同签订后支付合同价40%作为预付款，项目验收通过后支付到合同价的100%，具体付款方式双方协商确定。

**四、评标方法及标准**

**1、评标方法：**

本次评标采用综合评分法，投标文件满足采购文件全部实质性要求且按照评审因素的量化指标评审得分最高的供应商为中标候选人。得分相同的，投标报价低者为中标候选人。得分且投标报价相同的由采购人代表开标现场随机抽签确定。

**2.评分标准：**总分100分，其中商务技术分 70 分，价格分 30 分。下述所列为评分依据，分值如下（计算分值时，按其算术平均值保留小数2位）。

**01标商务技术分：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目 | 评分细则 | 分值 |
| 1 | 投标人资质 | 1.投标人通过ISO27001信息安全体系认证、ITSS 信息技术服务运行维护标准符合性肆级及以上认证。以上认证证明每提供一个得3分，共6分。2.投标人具有内网资产发现系统著作权证书、内网流量监控系统著作权证书、网站漏洞扫描系统著作权证书、服务器漏洞扫描系统著作权证书、等保检查资产审计指纹鉴别系统著作权证书，每提供一项著作权证书的得2分，最高得10分。**（提供证书复印件并加盖投标人公章，否则不得分）。** | 16 |
| 2 | 投标人同类项目业绩 | 根据投标供应商提供（2019年1月1日至今，以合同签订时间为准）同类项目业绩，1个业绩得1分，最高得3分。**（提供业绩合同复印件并加盖投标人公章，否则不得分）。** | 3 |
| 3 | 测评团队技术力量 | 1.投标人拟派的项目负责人具有高级信息安全等级测评师证书，并同时具有注册信息安全专业人员(CISP)、信息系统项目管理师（高级），每提供一本证书得3分，最高得9分，没有不得分。2.投标人拟派的项目技术负责人具有高级信息安全等级测评师证书、信息系统项目管理师（高级）、高级网络攻防技术与信息安全应急响应工程师、注册信息安全工程师CISP证书，每提供一本证书得2分，最高得8分，没有不得分。3.投标人拟派的项目团队人员中具有信息安全保障人员证书（CISAW）的技术人员每有一人得1分，最高得2分，没有不得分。4.投标人拟派的项目团队人员中具有中级信息安全等级测评师认证的技术人员每有一人得1分，最高得2分，没有不得分。5.投标人拟派的项目团队人员中具有初级信息安全等级测评师认证的技术人员每有一人得1分，最高得2分，没有不得分。**注：上述所有人员须为投标人在职职工，须提供投标人所属社保机构养老保险交纳清单（缴费单位和单位名称必须一致，并加盖社保缴费证明专用章）复印件并加盖公章，社保证明出具时间不得早于投标截止时间前3个月。** | 23 |
| 4 | 测评服务方案 | 根据投标人提供的测评服务方案由专家进行综合评定，服务方案应体现以下内容：1.项目方案针对性，完整性、可行性等优于项目需求的得4.1-6.0分，符合项目需求的得2.1-4.0分，基本符合项目需求的得0-2.0分。2.项目实施进度计划及合理性优于项目需求的得3.1-5.0分，符合项目需求的得1.1-3.0分，基本符合项目需求的得0-1.0分。3.方案体现项目组织实施、管理、措施等情况优于项目需求的得3.1-5.0分，符合项目需求的得1.1-3.0分，基本符合项目需求的得0-1.0分。。4.方案体现本项目的难点、要点和关键部位是否阐明优于项目需求的得3.1-4.0分，符合项目需求的得1.1-3.0分，基本符合项目需求的得0-1.0分。5.投标人是否根据自身经验对本项目的实施提出具有针对性的优化建议，其可行性如何优于项目需求的得2.1-3.0分，符合项目需求的得1.1-2.0分，基本符合项目需求的得0-1.0分。 | 23 |
| 5 | 培训和售后服务 | 根据售后服务承诺的范围和完善程度（包括技术支持、服务标准，测评及应急响应时间方式及保障措施，培训计划）综合打分，优于项目需求的得3.1-5.0分，符合项目需求的得1.1-3.0分，基本符合项目需求的得0-1.0分。 | 5 |

**注：所有证书都应在有效期内，逾期不得分。**

**01标价格分：**

2.2.1评标基准价：即满足采购文件要求且投标报价最低的投标报价为评标基准价，其价格分为满分。

2.2.2其他投标人的价格分统一按照下列公式计算：

投标报价得分=(评标基准价／投标报价)×价格权值×100

即：投标报价得分=(评标基准价／投标报价)×30