|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 扬州市中心血站关于网络安全等级保护测评工作项目询价单  YZRXXJ-2020092号 | | | | | | |
| （供应商）： 扬州仁信工程管理有限公司受扬州市中心血站的委托，要采购如下服务，请按下表格式报价并请注意如下事项： 1、所有报价均为人民币。 2、报价请于**2020年8月11日下午15：00**前密封并加盖供应商单位的公章送至扬州仁信工程管理有限公司（扬州市广陵区联谊路与开发东路交叉口东南角，苏高新名泽园南门10号商务楼二楼东），逾期或未予以密封或未加盖供应商单位的公章的将不予接收。 3、请将包括“单价”、“总价”在内的所有应填写的项目填全，否则以废单处理。 4、供应商如不按要求履行合同的，3年内不得进入扬州市政府采购市场，并根据《政府采购法》的规定予以处罚。  5、扬州仁信工程管理有限公司联系人：李清雯 13092036576；0514-82101606；  采购单位联系人姚主任0514-87959926。 | | | | | | |
| 报价表                   单位：元 | | | | | | |
| 序号 | 项目名称 | 单位 | 数量 | 单价(元) | 合价(万元) | 期限要求 |
| 1 | 网络安全等级保护测评工作 | 项 | 1 |  |  | 项目启动后30个自然日内完成等级保护测评并出具测评报告。 |
| 合计 | | | | ￥：     大写： | | |
| 供应商名称：（盖章） | | | |  | | |
| 联系人：电话号码： | | | | 年   月  日 | | |
| 报价要求 | | | | | | |
| 1、供应商参加政府采购活动应当具备的条件：符合《中华人民共和国政府采购法》第二十二条规定，具有独立法人资格及相应的经营范围。  2、报价具体事项：请在规定时间内一次性报出不得更改的价格。 3、参加本项目招标的供应商，在投标时须提供：(1)**营业执照（复印件加盖供应商公章）、**(2)**网络安全等级保护测评机构推荐证书（有效期内）(复印件加盖供应商公章，原件备查)、**(3)**法定代表人授权书（原件）和被授权人身份证（复印件）、**(4)**2017年以来所投项目类似合同壹份（复印件加盖供应商公章）。所有复印件加盖供应商公章。**未按要求提供材料或提供材料不全将不进入报价的评审。 4、报价供应商不得涂改询价单所有内容，否则当废单处理。本次招标预算价为**5.3万元**，超过预算价为无效报价。  5、报价中含：完成项目内容的全部费用-代理服务费（成交价\*1.2%，不足2000元则按2000元计收）-评审专家费（暂定900元，300元/位，按实结算，不提供发票）-售后服务-税金等费用。  **6、采购内容：在测评工作开展前，成交供应商须先对采购单位的网络系统进行整体预评估，判断是否存在风险。如存在风险，则应先出具书面的整改方案，采购人进行整改后，再进行预评估，直至风险完全消除，方可进行等级测评，评估结果必须为合格。**  7、成交供应商应提供优质的售后服务。  8、按照符合采购需求、质量和服务相等且报价最低原则确定成交供应商。  9、付款方式：项目内容完成且采购人取到等级保护证书，乙方开具合格发票，甲方一次性付清合同款。  10、其他注意事项：本项目仅接受当面递交投标书，不接受邮寄方式递交报价书。**投标保证金：壹仟元**（**开标现场以现金方式缴纳，现场查验，信封装好并注明单位名称**）  11、本询价采购单提供及公告期限：自询价公告在“扬州市中心血站网”发布之日起3个工作日。询价采购单在“扬州市中心血站网”上自行查阅，售价300元，报名时缴纳，售后不退。**供应商如确定参加询价，请如实填写《供应商参加询价确认函》**，打印后加盖公章，扫描或拍照发送至邮箱（yzrxgcgl@163.com）,报名接收（周日及法定节假日除外）截止时间：2020年8月7日下午23:59。《供应商参加询价确认函》原件请带至开标现场交代理公司工作人员。如供应商未按上述要求去做，将自行承担所产生的风险。有关本次招标的事项若存在变动或修改，敬请及时关注“扬州市中心血站网”发布的信息或变更公告。  12、服务需求及要求：详见本项目服务需求。 | | | | | | |

YZRXXJ-2020092号

扬州市中心血站关于网络安全等级保护测评工作项目服务需求

**一、项目背景**

等级保护是我国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）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”。2007年6月发布的关于印发《信息安全等级保护管理办法》的通知（公通字[2007]43号）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 号文件和43号文件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。

目前，国内国际信息安全形式非常严峻，我国各重要信息化基础设施面临的网络攻击、破坏、窃密等安全威胁日益增多，时刻威胁着我国的国家安全、社会秩序与公民利益。2014年2月中共中央成立了以习近平总书记为组长的中央网络安全和信息化领导小组，明确指出“没有网络安全就没有国家安全，没有信息化就没有现代化”。

根据《中华人民共和国网络安全法》、《信息安全等级保护管理办法》（公通字[2007]43号)、《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）、《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)等文件精神，扬州市中心血站拟于近期开展网络安全等级保护测评工作。

**二、项目依据**

1、政策依据

（1) 《中华人民共和国网络安全法》（2017年6月1日实施）

（2)《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)

（3)《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)

（4)《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)

（5)《信息安全等级保护管理办法》(公通字[2007]43号)

（6)《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)

（7)《信息安全技术 信息系统安全等级保护实施指南》(GB/T 25058-2010)

（8)《计算机信息系统安全保护等级划分准则》(GB 17859-1999 )

（9)《信息安全技术信息系统安全等级保护定级指南》(GBT 22240—2008)

（10)《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303号）

2、技术标准

（1） 《信息安全技术 信息系统安全等级保护基本要求》（GBT 22239-2008）

（2) 《信息安全技术信息系统安全等级保护测评要求》(GB/T 28448-2012)

（3) 《信息安全技术信息系统安全等级保护测评过程指南》(GB/T 28449-2012)

（4） 《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）

（5） 《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）

（6） 《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）

（7） 《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）

（8） 《信息安全技术 终端计算机系统安全等级技术要求》（GA/T671-2006）

（9） 《信息安全技术 信息系统安全管理要求》（GB/T 20269—2006）

（10) 《信息安全技术 信息系统安全管理测评》（GA/T 713-2007）

（11） 《信息技术 安全技术 信息安全管理体系要求》（GB/T22080-2008）

（12） 《信息技术 安全技术 信息安全管理实用规则》（GB/T22081-2008）

**三、项目原则**

1、客观性原则

测评人员应当没有偏见，在最小主观判断情形下，按照双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

2、连续性原则

确保在高速变化的信息安全环境中，在有效的服务期间内，保证采购人测评结论的准确性和及时性，对于采购人单位新增设的信息资产和服务，或新建立的信息化项目，进行局部系统的重新评估。

3、扩展性原则

在测评过程结束后，信息安全测评过程要保持扩展性，从扩展的属性上进一步加强测评结束后采购人的安全管理有效性和可用性。

4、保密原则

在测评过程中，需严格遵循保密原则，双方签订保密协议，对服务过程中涉及到的任何用户信息未经允许不向其他任何第三方泄漏，以及不得利用这些信息损害采购人利益。

5、互动原则

在整个测评过程中，强调采购人的互动参与，每个阶段都能够及时根据采购人的要求和实际情况对测评的内容、方式做出相关调整，进而更好的进行测评工作。

6、最小影响原则

测评工作应该尽可能小地影响系统和网络的正常运行，不能对业务的正常运行产生明显的影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应做出说明。

7、规范性原则

信息安全测评的实施必须由专业的测评服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，并提供完整的服务报告。

8、质量保障原则

在整个测评过程中，须特别重视项目质量管理。项目的实施将严格按照项目实施方案和流程进行，保证项目的进度和质量。

**四、项目内容**

在测评工作开展前，成交供应商须先对采购单位的网络系统进行整体预评估，判断是否存在风险。如存在风险，则应先出具书面的整改方案，采购人进行整改后，再进行预评估，直至风险完全消除，方可进行等级测评，评估结果必须为合格。

本次项目共涉及信息系统为扬州市中心血站内所有信息系统。

根据各信息系统的安全保护等级，依据国家等级保护相关标准，通过信息安全等级保护测评的方法，查找信息系统各安全层面与相应安全保护等级标准的差距，明确存在的安全问题，提出书面的整改方案，然后再进行预评估，直至风险完全消除，方可进行等级测评，编制提交《信息系统安全等级测评报告》报告结果须为合格，并以此报告指导后续的安全整改。

具体工作内容如下：

1、信息收集：对项目涉及的所有信息系统开展调研工作，明确所有系统的物理环境及机房基础设施情况，网络架构，网络设备、安全设备部署情况，服务器分布及操作系统、数据库系统使用情况，应用系统业务流程、数据流向、用户群体情况，数据传输及存储备份情况，系统的高可用性需求情况，安全管理制度建设及执行情况。

2、方案编制：根据收集的基础信息，识别各信息系统网络结构及其网络覆盖范围、系统构成，明确测评目的及流程、明确测评对象及指标、明确测评方法及工具扫描接入点、明确测评实施步骤及配合需求、明确测评实施计划。并据此编制《测评方案》、开发《测评指导书》。

3、现场实施：依据《测评方案》、参照《测评指导书》，通过访谈、检查、测试、实地查看等方法开展现场测评活动，详细记录每个测评对象的安全现状，形成《现场测评记录表》。

4、汇总分析：根据现场测评记录，按照物理安全、网络安全、主机安全、应用安全、数据安全、安全管理几个安全层面，汇总各安全层面测评对象的安全现状，形成《安全问题汇总表》。

5、问题交流：通过交流会的形式，对《安全问题汇总表》中的内容进行沟通交流，明确安全问题是否真实存在，如有遗漏或不确定项需进行补充测评并详细记录结果。

6、报告编制：对现场测评结果进行汇总分析、整体测评、风险评价，提出建设整改建议，直至风险完全消除后，再给出等级测评结论，编制、评审、提交《信息系统安全等级保护测评报告》。

**五、项目要求**

1、项目实施过程中，投标人如需采购人配合，投标人需要详细描述需要配合的内容。

2、投标人应配置有经验的测评工程师进行本项目的服务工作，在确定项目组人员组成后未经采购人确认不允许随意更换。

3、本项目中可能需要的软硬件平台(如笔记本电脑、测试软件等)均由成交人提供，采购人可按照相关要求对设备进行必要的处理。投标人在服务期间未经采购人许可不得使用任何未经确认的存储设备对测评数据进行复制。投标人必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由投标人负完全责任。

4、投标人需要给出在进行调研时所需要提供的信息列表。采购人有权利拒绝提供任何信息列表以外的采购人资产信息。

5、成交人应向各提供详细的测评材料、各种表单及结果报告。

6、测评工作的范围、内容、形式、标准等，应符合国家及行业的有关标准及规范要求。

7、测评期限要求：项目启动后30个自然日内完成等级保护测评并出具测评报告。