查看项目

返回

项目状态： 已成交

项目结果

排名	供应商名称	报价（元）	报价时间	成交结果
1	广州理想资讯科技有限公司	136,800.00	2022.07.25 09:47:50	成交
2	广州领慧信息科技有限公司	138,000.00	2022.07.25 09:44:53	未中标
3	广州市欧驰信息技术有限公司	139,100.00	2022.07.25 09:23:17	未中标

采购计划

定点品目: 测试评估认证服务

采购计划: 急救系统和MDT多学科联合诊治系统三级等保

计划编号: 440101-2022-16215

计划品目: 测试评估认证服务

计划金额: 140,000.00元

项目信息

项目名称: 广州市第一人民医院信息技术服务（广州集采）定点采购

采购单位: 广州市第一人民医院

预算金额: 140,000.00 元

报价截止时间: 2022-07-25 16:00

联系人: 陈志刚

联系电话: 19124386003

收货地址: 广东省-广州市-越秀区广东省广州市越秀区盘福路1号

支付方式: 3.其他支付方式（1）第一笔款项支付：合同签订生效后，采购人在收到中标人款项发票及相关资料后30个工作日内，采购人向中标人支付合同总价的30%款项。（2）第二笔款项支付：完成信息系统定级备案后，采购人在收到中标人款项发票及相关资料后30个工作日内，采购人向中标人支付合同总价的30%款项。（3）第三笔款项支付：完成信息系统等级保护测评服务并获得提交网络安全等级测评报告回执后，采购人在收到中标人款项发票及相关资料后30个工作日内，采购人向中标人支付合同总价的40%款项。（4）付款凭证资料：合同复印件；开具的正式发票；验收报告（加盖科室章）。

需求信息

合同份数：4

争议处理方式：向人民法院提交诉讼解决

需求明细

序号	服务描述	需求描述	数量
1	服务内容：本项目主要为医院提供急诊急救系统和MDT多学科联合诊治系统进行信息系统定级备案、网络安全等级保护差距安全评估、网络安全等级保护安全加固、网络安全等级保护验收测评服务等服务。要求合格的报价人提供满足上述需求的服务，且用于完成上述服务所需要的一切工具和软件等由投标人自行提供。（1）定级备案服务 根据《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 网络安全等级保护定级指南 GB/T 22240-2020》等相关标准，中标人需在合同签订后1个工作日内开展定级备案工作，填写备案材料，组织专家定级评审（医院不单独支付专家评审时产生的费用），提交备案材料至公安部门。（2）网络安全等级保护差距安全评估服务 中标人在系统定级备案成功后1个工作日内，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过程指南》GB/T 28449-2018、《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 网络安全等级保护测评要求》GB/T 28448-2019、《信息安全技术 网络安全等级保护安全设计技术要求》GB/T25070-2019等有关要求进场开展网络安全等级保护安全评估服务，评估内容包括本单位定级系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心5个技术层面；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5个管理层面进行现场测评和差距分析，记录相关的测评结果，输出现场测评记录结果。 依照《等级保护现场测评记录》中所记录的针对本单位定级系统的技术和管理测评结果，结合系统整体差距评估结果，按照公安部标准测评报告模板撰写测评记录，完成现场差距测评后提交《系统问题清单》。（3）网络安全等级保护安全加固服务 按照《网络安全等级保护三级信息系统》要求进行整改，针对《系统问题清单》的不符合项进行安全加固工作，每周跟踪整改结果并现场书面汇报，向医院反馈清晰的整改进度；对操作系统漏洞的修复工作，应确保修复后的系统环境能够正常	用户需求书 一、项目名称：急诊急救系统和MDT多学科联合诊治系统三级等保服务项目 二、资格要求/供应商资格门槛 1.符合《中华人民共和国政府采购法》第二十二条规定的条件，提供下列材料：（1）具有独立承担民事责任的能力，分支机构投标的，需提供分支机构的营业执照（执业许可证）扫描件及总公司（总所）出具给分支机构的授权书。（2）有依法缴纳税收和社会保障资金的良好记录。（3）具有良好的商业信誉和健全的财务会计制度。（4）履行合同所必需的设备和专业技术能力。（5）参加采购活动前3年内，在经营活	1

运作，发挥系统软件应有的功能。整改前做好实施方案及计划，整改期间必须做好各项保障措施，确保医院信息系统的稳定性，不得影响医院的正常业务运行，如不按照相关要求给医院造成损失的，由中标人承担。 对除操作系统以外的应用中间件、数据库、业务系统应用程序的漏洞，出具安全漏洞整改建议，及时通知相关业务系统管理员，并在整改过程中提供相应的技术指导。 在充分参考ISO27001、国家网络安全等级保护等国内外先进的安全标准的前提下，建立一套切实可行的安全管理体系，增加医院个人信息保护方面的管理制度，加强安全管理机制。 （4）网络安全等级保护验收测评服务 在信息系统完成安全加固后，对信息系统的安全技术和安全管理上各个层面的安全控制进行整体性验证，使医院的信息系统达到网络安全等级保护的安全要求。完成测评工作后，需在7个工作日内出具《验收测评报告》，提交至广州市公安网监，并获得公安网监开具的备案证明和验收测评报告签收的回执文件。
需求详细说明:查看附件

动中没有重大违法记录。 2.落实政府采购政策需满足的资格要求：本项目不属于专门面向中小微企业采购的项目。 3.本项目特定的资格要求：（1）本项目不接受联合体投标。 （2）供应商未被列入“信用中国”网站中“记录失信被执行人或重大税收违法案件当事人名单或政府采购严重违法失信行为”的记录名单；不处于“中国政府采购网”中“政府采购严重违法失信行为信息记录”的禁止参加政府采购活动期间。 （3）供应商必须符合法律、行政法规规定的其他条件。 三、项目实质性条款一览表 序号 实质性条款 备注 1 ★本次采购产品为非进口产品（进口产品指通过中国海关报关验放进入中国境内且产自关境外的产品）。 四、详细采购需求 1、 项目基本概况介绍 为贯彻和落实《中华人民共和国网络安全法》、《关于落实网络安全保护重点措施深入实施网络安全等级保护制度的指导意见》（公网安[2022]1058号）等法律、法规、政策文件的要求，我院拟开展信息系统网络安全等级保护测评和整改服务，从物理环境、通信网络、区域边界、计算环境及安全管理等各方面进行的网络安全检测评估。 本次需完成网络安全等级保护测评和整改的信息系统如下： 序号 信息系统名称 系统级别 备注 1. 急诊急救系统 三级 2. MDT多学科联合诊治系统 三级 2、 采购内容 (一) 采购清单 标的名称 数量 服务期限 备注 急诊急救系统和MDT多学科联合诊治系统等保测评服务 1 自合同签订之日起90天内 (二) 符合的国家相关标准、行业标准、地方标准或者其他标准、规范 《中华人民共和国网络安全法》 《中华人民共和国数据安全法》 《中华人民共和国个人信息保护法》 《关于印送<关于落实网络安全保护重点措施深入实施网络安全等级保护制度的指导意见>的函》（公网安[2022]1058号）《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 网络安全等级保护定级指南》GB/T 22240-2020 《信息安全技术 网络安全等级保护测评过程指南》GB/T 28449-2018 《信息安全技术 网络安全等级保护实施指南》G

B/T 25058-2019《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 网络安全等级保护实施指南》GB/T25058-2019《信息安全技术 网络安全等级保护安全设计技术要求》GB/T25070-2019 卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知卫办发[2011]85号 3、 服务内容 本项目主要为医院提供急诊急救系统和MDT多学科联合诊治系统进行信息系统定级备案、网络安全等级保护差距安全评估、网络安全等级保护安全加固、网络安全等级保护验收测评服务等服务。要求合格的报价人提供满足上述需求的服务，且用于完成上述服务所需要的一切工具和软件等由投标人自行提供。（1）定级备案服务 根据《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 网络安全等级保护定级指南 GB/T 22240-2020》等相关标准，中标人需在合同签订后1个工作日内开展定级备案工作，填写备案材料，组织专家定级评审（医院不单独支付专家评审时产生的费用），提交备案材料至公安部门。（2）网络安全等级保护差距安全评估服务 中标人在系统定级备案成功后1个工作日内，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过程指南》GB/T 28449-2018、《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 网络安全等级保护测评要求》GB/T 28448-2019、《信息安全技术 网络安全等级保护安全设计技术要求》GB/T25070-2019等有关要求进场开展网络安全等级保护安全评估服务，评估内容包括本单位定级系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心5个技术层面；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5个管理层面进行现场测评和差距分析，记录相关的测评结果，输出现场测评记录结果。 依照《等级保护现场测评记录》中所记录的针对本单位定级系统的技术和管理测评

结果，结合系统整体差距评估结果，按照公安部标准测评报告模板撰写测评记录，完成现场差距测评后提交《系统问题清单》。（3）网络安全等级保护安全加固服务 按照《网络安全等级保护三级信息系统》要求进行整改，针对《系统问题清单》的不符合项进行安全加固工作，每周跟踪整改结果并现场书面汇报，向医院反馈清晰的整改进度；对操作系统漏洞的修复工作，应确保修复后的系统环境能够正常运作，发挥系统软件应有的功能。整改前做好实施方案及计划，整改期间必须做好各项保障措施，确保医院信息系统的稳定性，不得影响医院的正常业务运行，如不按照相关要求给医院造成损失的，由中标人承担。 对除操作系统以外的应用中间件、数据库、业务系统应用程序的漏洞，出具安全漏洞整改建议，及时通知相关业务系统管理员，并在整改过程中提供相应的技术指导。 在充分参考ISO27001、国家网络安全等级保护等国内外先进的安全标准的前提下，建立一套切实可行的安全管理体系，增加医院个人信息保护方面的管理制度，加强安全管理机制。（4）网络安全等级保护验收测评服务 在信息系统完成安全加固后，对信息系统的安全技术和安全管理上各个层面的安全控制进行整体性验证，使医院的信息系统达到网络安全等级保护的安全要求。完成测评工作后，需在7个工作日内出具《验收测评报告》，提交至广州市公安网监，并获得公安网监开具的备案证明和验收测评报告签收的回执文件。 4、服务总体要求和具体要求 在网络安全等级保护测评过程中，应采用询问、检查、测试、工具扫描等多种手段组合的方式。工具扫描应至少包括使用：安全评估系统(即安全脆弱性扫描)工具对重要服务器、网络设备、部分客户端（5%-10%）进行漏洞扫描。报价人须在投标文件中列出安全评估系统(即安全脆弱性扫描)工具，并说明设备的最终归属权，为规避可能带来的法律风险，若非原生产厂家，需在中标后1个工作日提供安全评估系统(即安全脆弱性扫描)工具原生产厂家关于本项目的产品授权函。若引起

任何知识产权或者相关法律纠纷，由中标人承担责任并补偿因此对医院造成的损失。所提供用于安全评估系统(即安全脆弱性扫描)工具和安全配置核查工具应至少包含或高于以下工具指标要求，原生产厂家需提供相关的截图证明材料： 1）支持检测的漏洞数大于150000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，并提供CVE Compatible证书。 2）产品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。 3）提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。 4）内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术。 5）具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。 6）支持和微软WSUS补丁系统的联动，能够在发给主机管理员的邮件中附带自动配置WSUS的注册表文件，方便进行自动化的补丁修补。 7）支持扩展配置核查功能、web漏洞扫描功能，并在同一界面、同一账号实现登录，并同一报表上展现漏洞扫描结果和配置核查结果，非采用单点登录方式或非三种系统（将系统漏扫、配置核查系统、web漏扫系统集成在一台设备上，三个独立界面）方式实现。 8）支持将按IP范围、起止时间、任务名称、任务状态、漏洞模板、用户等筛选扫描任务,并对筛选结果进行汇总,和生成在线及离线报表。 9）产品要求取得公安部颁发的《计算机信息系统安全专用产品销售许可证(增强级)》，提供产品有效证书的复印件。 5、 服务质量要求/或技术指标要求 （1）项目建设工期要求：自合

同签订之日起90天内，中标人应通过自身在等保测评工作中积累的经验，结合自身的技术优势，充分考虑到信息系统实际情况，根据项目阶段要求提供一份具体细致的、操作性强的网络等保测评和整改实施计划，并按照医院的要求完成信息系统等级保护的相关工作，取得监管单位开具的备案证明或验收测评报告签收回执文件。如不按照相关要求在约定工期内完成服务给医院造成损失的，由中标人承担违约责任。（2）中标人应通过在安全技术和安全管理上选用与安全等级相适应的安全控制来实现信息系统安全等级。做到不同安全等级的信息系统应具有不同的安全保护能力，并使信息系统安全等级保护达到信息系统安全等级保护工作的各项要求。 6、 交付使用要求 本项目需要按照等保2.0的流程要求，结合当前、信息系统安全建设的实际情况进行总体设计，并把整个项目分成以下4个阶段。 项目阶段表 阶段 实施内容 产出物 等保差距测评 现场评测阶段通过与评测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。现场测评工作应取得报告编制活动所需的、足够的证据和资料 差距测评问题清单 等保整改 参照《差距测评问题清单》乙方指导甲方完成网络设备基线配置、网络安全设备基线配置、操作系统基线配置、操作系统补丁修复、数据库配置、管理制度文档。 整改记录 等保验收 渗透测试复测，测评机构应对现场测评获得的测评结果进行汇总分析，形成等级测评结论。《网络安全等级保护测评报告》 项目完成 将系统验收测评报告提交至广州市公安网监部门。 获得提交网络安全等级测评报告回执 7、设备及产品安装、测试及验收标准及要求 中标人完成急诊急救系统和MDT多学科联合诊治系统的网络安全等级保护工作，包括：信息系统定级备案、网络安全等级保护差距安全评估、网络安全等级保护安全加固、网络安全等级保护验收测评，并获得公安部门出具的提交网络安全等级测评报告回

执，上述工作完成后视为项目终验。 8、 人员要求 （1）为保障项目进度和质量，所有参与测评人员需具备信息系统等级保护测评工作经验，精通等级保护测评技术，能分析测评过程中存在的风险。中标人需安排1名项目经理负责项目质量把控，1名技术服务人员提供为期2个月的5*8的驻场服务，负责等级保护全过程的支撑及风险整改跟进工作。在中标后提供驻场人员的经验和资质要求供采购人审核，如不符合要求，视为无效报价。 项目经理要求如下： 本科或以上学历，计算机相关专业，网络安全工作经验10年以上，具备CISP注册信息安全专业人员认证、CISP-DSG注册数据安全专业人员认证、系统集成项目管理工程师或项目管理师认证。驻场人员技能、经验、学习能力和学历要求如下： 本科或以上学历；具备CISP注册信息安全专业人员、信息网络安全专业技术人员（信息安全等保类）、助理工程师（专业方向：网络空间安全系统测评） 具有对信息系统所面临的安全威胁、存在的安全隐患进行信息收集、识别、分析和提供防范措施的能力。 具有能根据用户信息系统安全防护问题的分析，向用户建议有效的安全保护策略及建立完善的安全管理制度的能力。 具有对发生的突发性安全事件进行分析和解决的能力。应了解、掌握并能应用等级保护测评国家和行业标准，需根据等级保护测评工作中发现的安全隐患，提供详细的安全加固建议报告。（2）服务人员工资不得低于广州市企业职工最低工资标准（工资不含服务商按国家规定必须为服务人员支付的社会保险及其他应付费用）。（3）服务人员薪金要求按广州市劳动用工相关标准执行，请服务商充分考虑服务期内人员薪金的调整因素，如因用工引起的劳动纠纷问题由服务商负责解决。（4）我院对岗位设置、人员选用与日常管理具有监督权和协调权。服务商必须保证派驻服务人员的稳定性，如有工作人员调离，需书面通知我院。由于派驻的服务人员不尽忠职守或我院认为不符合要求的，服务商必须在接到书面通知后3天内无条件更换人员。（5）服务商工作

人员须遵守我院相关规章制度规定，如有违反或损害我院利益的，我院有权拒绝违规的工作人员在此工作，问题严重的，我院有权终止合同，一切责任由服务商承担。（6）为确保工作的质量，驻点人员在服务期间未经招标方同意不得随意更换，如果中途更换，中标人必须征得我院同意，并支付10000元/次误工费。 9、 售后服务要求 报价人需对以下内容进行承诺：（1）针对本次项目服务文档的知识产权归属医院所有，报价人原有产品既有知识产权不因本项目发生转移，涉及到第三方提出侵权或知识产权的起诉及支付版税等费用由报价人承担所有责任及费用。（2）医院为报价人提供的所有业务、技术资料，报价人有责任对第三方保密。如未经采医院书面同意，擅自将涉及医院商业和技术秘密的资料透漏给第三方，医院将保留追究投标人法律责任的权利。 10、 培训要求 为了使医院的信息系统管理人员掌握等保的标准，要求提供等保标准的培训：（1）培训：提供对系统管理人员培训。（2）培训目标：相关人员经培训后能掌握等保的标准。（3）培训方式和操作使用手册：投标人应提供详细的培训计划，具体培训时间、地点以用户认可为准，投标人须提供培训PPT、标准电子文件等培训材料，方便学习和使用。（4）必须派出具有相应专业资格和实际工作经验的技术人员进行培训，并承担本项目的所有培训费用。 11、 付款方式（1）第一笔款项支付：合同签订生效后，采购人在收到中标人款项发票及相关资料后30个工作日内，采购人向中标人支付合同总价的30%款项。（2）第二笔款项支付：完成信息系统定级备案后，采购人在收到中标人款项发票及相关资料后30个工作日内，采购人向中标人支付合同总价的30%款项。（3）第三笔款项支付：完成信息系统等级保护测评服务并获得提交网络安全等级测评报告回执后，采购人在收到中标人款项发票及相关资料后30个工作日内，采购人向中标人支付合同总价的40%款项。（4）付款凭证资料：合同复印件；开具的正式发票；验收报告（加盖科室章）。

商务需求

序号	需求描述
1	在网络安全等级保护测评过程中，应采用询问、检查、测试、工具扫描等多种手段组合的方式。工具扫描应至少包括使用描。报价人须在投标文件中列出安全评估系统(即安全脆弱性扫描)工具，并说明设备的最终归属权，为规避可能带来的法于本项目的产品授权函。若引起任何知识产权或者相关法律纠纷，
2	由中标人承担责任并补偿因此对医院造成的损失。所提供用于安全评估系统(即安全脆弱性扫描)工具和安全配置核查工具于150000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，并提供CVE Compatible证书。
3	2）产品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、M器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。
4	4）内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描B、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行
5	6）支持和微软WSUS补丁系统的联动，能够在发给主机管理员的邮件中附带自动配置WSUS的注册表文件，方便进行自同一报表上展现漏洞扫描结果和配置核查结果，非采用单点登录方式或非三种系统（将系统漏扫、配置核查系统、web漏
6	8）支持将按IP范围、起止时间、任务名称、任务状态、漏洞模板、用户等筛选扫描任务,并对筛选结果进行汇总,和生成在提供产品有效证书的复印件。
7	项目经理要求如下： 本科或以上学历，计算机相关专业，网络安全工作经验10年以上，具备CISP注册信息安全专业人员
8	为确保工作的质量，驻点人员在服务期间未经招标方同意不得随意更换，如果中途更换，中标人必须征得我院同意，并支
9	针对本次项目服务文档的知识产权归属医院所有，报价人原有产品既有知识产权不因本项目发生转移，涉及到第三方提出

采购规则

定点规则： 定点竞价 查看规则详情