**扬州大学附属医院信息化提升工程二期云资源与安全租赁项目院内公开谈判文件**



采 购 人：**扬州大学附属医院**

发 放 日 期：**2024年6月**

**目 录**

一、招标邀请………………………………………………………………………2

二、项目需求………………………………………………………………………3

三、投标人须知……………………………………………………………………7

四、投标文件格式及附件要求……………………………………………………9

五、供应商廉洁自律承诺书………………………………………………………14

**一、招标邀请**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 项目名称 | **扬州大学附属医院信息化提升工程二期云资源与安全租赁项目** | | | | |
| 服务地点 | **扬州大学附属医院** | | | | |
| 承包方式 | / | 质量标准 | | 合 格 | |
| 院内公开谈判预算 | 29万/3年 | 标书工本费 | | / | |
| 投标文件要求 | 投标文件正本1份，副本4份；所有投标文件的封面及封袋上都必须加盖投标单位法人公章及其法定代表人或授权委托人的签字。 | | | | |
| 报名截止时间 | 2024年6月17日17：00 | | | | |
| 文件递交地址 | 扬大附院西区行政楼403办公室 | | | | |
| 开标时间 | **2024.6.18 14：30** | | 地点 | | **扬大附院西区行政楼407室** |
| 联系方式 | 联系人：张老师 联系电话：0514-82099552  地址：扬大附院西区行政楼403办公室 | | | | |
| 备注 | **未提供格式的投标人自拟。** | | | | |

**二、项目需求**

1. **项目背景**

依据医院信息化建设规划，2024年医院实施“信息化提升工程二期”建设，为满足未来信息化发展需求，现对医院“云资源与云安全”建设内容进行规划与建设。本项目以本次云资源应用需求为基础，结合未来医院信息化建设需求，不断完善医院云资源与云安全管理体系。

项目建设应充分体现医疗业务服务的连续性、医疗信息的安全性、政策的合规性等行业特点。本项目为交钥匙项目，投标报价应含所有采购供货及需要安装调试的各分项建设内容所需的费用，投标人应充分考虑到完成项目所需要的人力资源，辅材及投入及各项措施所产生的费用，并包含在投标总价中。采购人将不予额外支出完成项目所需的其它费用，包括人工、运输、安装、辅材及其它一切与本项目相关的衍生费用。

本项目预算价：***29万元（三年服务期总费用），报价时报一年期费用。***

服务期及付款方式：服务期三年，合同一年一签。在年度评分考核合格及双方无异议情况下续签下一年度服务合同。合同采用后付费方式，即年度服务期满，服务质量合格的情况下，凭开具的发票付款。

1. **建设目标**

建设信息化提升工程二期应用项目云资源：依据医院信息化提升工程二期建设内容提供云资资源与云安全管理，满足医院二期云应用部署要求（具体需求见建设内容）。

完善医院云资源与云安全管理体系：充分考虑项目二期建设需求及未来医院信息化发展对云资源与云安的全管理需要，具备多套安全产品协同、高效资源利用、平滑升级、灵活扩展、部署便捷等性能。

逐步迁移医院原有云资源的应用，实现医院外网、内外网交互等应用的统一安全管理。

满足网络安全等级保护2.0三级（下简称等保三级）信息安全管理要求。

具备配合医院互联网IPv6规模部署升级改造实施的能力。

为保证医疗数据安全性和合规性，要求业务部署机房需在扬州市区或扬州本地。

1. **政策依据**

项目建设应满足以下标准

1、《国家健康医疗大数据标准、安全和服务管理办法》国卫规划发〔2018〕23号

2、《江苏省卫生信息化项目建设网络安全管理规定（试行）》苏卫办规划【2022】2号；

3、《关于做好互联网应用IPv6升级改造工作的通知-江苏省IPv6规模部署升级改造实施指南》扬卫规划函【2022】1号；

4、《信息安全等保护管理办法》、《商用密码应用安全性评估管理办法》等规定；

1. **建设内容**

**1、建设清单**

本次项目云资源与云安全应包括以下内容。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **内容** | **名称** | **配置要求** | **数量** |
| 1 | 互联网应用服务云资源 | 新网站服务器（主、备） | 4核8G，硬盘不低于300G/ Linux操作系统，1年服务，见详细技术指标要求。 | 2 |
| 老网站服务器 | 4核8G/500GB数据盘（SSD）/正版操作系统、版本为WindowsServer2012，1年服务，见详细技术指标要求。 | 1 |
| mmc前置机 | 4核8G/200GB高效云盘/正版操作系统、版本为Windows Server 2008 R2 企业版 64位中文版，1年服务，见详细技术指标要求。 | 1 |
| 网站一预约平台一nginx | 4核8G/200GB高效云盘/操作系统：CentOS 7.2 64位，1年服务，见详细技术指标要求。 | 1 |
| 短信平台 | 4核16G/200GB高效云盘/操作系统：CentOS 7.2 64位，1年服务，见详细技术指标要求。 | 1 |
| 支付平台 | 2核8G/200GB高效云盘/操作系统：CentOS 7.2 64位，1年服务，见详细技术指标要求。 | 1 |
| 小程序（病案打印） | 2核8G /200GB高效云盘/操作系统：CentOS 7.2 64位，1年服务，见详细技术指标要求。 | 1 |
| 负载均衡 | 100M带宽(主备，支持IPV6)，1年服务，见详细技术指标要求。 | 2 |
| 2 | 互联网应用云安全资源（包括但不限于） | 堡垒机 | 用于集中管理资产访问权限，为运维人员提供统一、高效、安全的运维通道，可提供运维身份鉴别、账号管控、系统操作审计等多种功能。1年服务。 | 1 |
| 防火墙 | 云环境下租户网络边界的下一代防火墙，具有统一管理互联网到云业务主机的精细化访问控制、高效威胁防护和高级威胁检测等功能。1年服务。 | 1 |
| 数据库审计 | 针对数据库系统的安全审计产品，对来自应用系统客户端和DBA对数据库的访问行为进行全面审计，对SQL注入、危险操作进行记录和实时预警、及时阻止，从而达到保护数据库的良好效果。1年服务。 | 1 |
| Web网站安全防护 | 对网站或者APP的业务流量进行恶意特征识别及防护，将正常、安全的流量回源到服务器。避免网站服务器被恶意入侵，保障业务的核心数据安全，解决因恶意攻击导致的服务器性能异常问题。具备Web安全防护、DDoS攻击防护、CC防护等。1年服务，见详细技术指标要求。 | 1 |
| SSL证书 | 网站和移动应用（APP）及小程序提供数据HTTPS加密协议访问，保障数据的安全。装载SSL证书产品后自动激活浏览器中显示“锁”型安全标志，地址栏以“https”开头。1年服务，见详细技术指标要求。 | 1 |
| 主机安全 | 主机安全是集防病毒、防火墙、入侵防御于一体的主机安全解决方案，旨在解决虚拟化环境下虚拟主机的病毒风险、攻击风险、管理风险及宿主主机的安全等一系列的安全问题。1年服务，见详细技术指标要求。 | 8 |
| 3 | 线路租用 | 互联网线路 | 100M带宽(主备，支持IPV6)，1年服务，见详细技术指标要求。 | 2 |
| 院内网络线路 | 可选实体VPN或专线打通医院内网。100Mbps带宽以上（主、备），1年服务。 | 2 |
| 4 | 安全服务 | 云资源安全运营服务 | 提供云上业务的安全防护与闭环处置，确保业务的安全、稳定与连续性运营。  （1）通过**专职专属服务经理与技术专家团队**提供7\*24小时全年无间断的监测、分析与响应服务；  （2）**提供云态势感知平台和威胁狩猎服务**包括：①.接入设备情况；②.总体安全评级，并可自定义评级规则；③.业务风险总览、资产风险总览；④.资产感知情况；⑤.热点事件发生情况；（3）**提供业务上线评估服务**，对需要上云部署的业务系统进行资产梳理、漏洞发现等安全风险评估。 | 1 |
| 渗透服务 | 每年提供3个业务系统，渗透测试服务，1年服务。见详细技术指标要求。 | 1 |

**2、详细技术指标要求**

## （1）互联网应用服务云资源

|  |  |
| --- | --- |
| **名称** | **指标参数要求** |
| 云服务器 | （1）按照配置要求提供不少于8台通用型云服务器，总资源量≥28vCPU，72G内存，3100G数据盘；  （2）支持基础配置变更，可进行实例的vCPU、内存、系统盘、数据盘等配置的增加和减少；  （3）支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员；提供产品功能截图。  （4）支持条带化功能，并且支持以虚拟磁盘为单位设置不同的条带数；  （5）▲为保证磁盘健康，支持坏道扫描功能，可以通过设置定时坏道扫描任务（启用/关闭）进行磁盘修复和坏道预测，可以自行设置定时坏道扫描任务中的执行时间。支持磁盘坏道预测，在界面可以查看磁盘坏道预测页面信息、包括坏道预测、坏道扫描和坏道数据修复。可以查到磁盘坏道列表项信息，包括硬盘名称、坏道预测、最近7天坏道扫描、坏道数据修复和硬盘风险状态；**（需提供第三方权威测试机构的证明材料，至少包含报告首页，对应功能测试页和报告尾页，加盖原厂公章）**  （6）当硬盘处于亚健康状态时，支持手动隔离硬盘，并将硬盘上的数据迁移至健康的硬盘上，即使更换系统盘仍不影响业务控；  （7）1年租用服务 |
| 负载均衡 | （1）吞吐≥500M，并发连接数≥1000000，支持IPV6；  （2）基础架构采用集群部署，保证服务的稳定性；  （3）▲支持模拟健康监测功能，无需完成真实的业务配置即可提前采用icmp、http、https、tcp、ftp、MYSQL、LDAP以及dns等的健康检查方式模拟检查业务的健康状态；**（提供国家信息安全测评中心、公安部信息安全产品检测中心、中国泰尔实验室任一家国家权威机构相关证明材料或提供封面具有“CMA”或“CNAS”标识的检测报告，并加盖原厂公章）**  （4）支持多种链路检测方法，能够通过PING、TCP、HTTP等方式监控链路的连通性，当某一条链路故障时，可将访问流量切换到其它链路，保障业务的持久通畅；  （5）内置完备的IP地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能；  （6）支持配置每台的服务器最大连接限制和新建连接限制，以及单个特定用户或者一个用户组中所有用户访问指定应用服务的并发连接总数限制，避免应用系统的服务器过载；  （7）支持自定义服务器端SSL协议策略(比如SNI)加密流量，可根据需求设置更精细的加密策略；**（提供第三方检测报告，并加盖原厂公章）**  （8）1年租用服务 |

## （2）互联网应用云安全资源

|  |  |
| --- | --- |
| **名称** | **指标参数要求** |
| 堡垒机 | （1）可管理设备数量不少于10个。  (（2）堡垒机支持采用高可用架构部署，保证各项服务正常运维。  **(（3）**▲支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。**（提供产品功能截图，并加盖原厂公章）**  (（4）支持命令黑命单，对字符型设备（如linux/unix/网络设备）的高危命令执行进行阻断，如rm、shutdown、reboot等。  (（5）支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断。  **(**（6）支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人。提供产品功能截图，并加盖厂商公章。  (（7）支持手动和自动定期备份配置信息，支持配置信息本地备份及异地FTP备份，支持系统配置还原，可以还原至任一备份点。  **(（8）**▲所投产品的生产厂商同时为国家信息安全漏洞共享平台(CNVD)技术组和用户组成员产品。**（提供证明材料并加盖原厂公章）**  **1**（9）1年租用服务 |
| 防火墙 | 1. 配套满足业务要求的防火墙组件，包含防病毒和IPS的能力，带宽性能≥100M。 2. 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 3. 内置海量互联网URL分类库，支持过滤上千万条恶意URL。 4. ▲产品内置不低于13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。**（提供产品功能截图，并加盖原厂公章）** 5. 具备访问控制功能，支持基于区域、IP地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。 6. 支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。 7. 产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过120万种，可识别主机的异常外联行为。（提供产品功能截图，并加盖厂商公章） 8. 支持在单条安全策略中可同时启用入侵防御、URL过滤、文件过滤等安全功能。 9. 为保障产品软件的成熟度，要求所投产品的生产厂商具备中国网络安全审查技术与认证中心CCRC的软件安全开发服务资质（二级及以上）（提供证明材料并加盖厂商公章） 10. ▲近年来医疗行业勒索病毒事件频发，为保障我院本次上云业务的安全性，产品需支持勒索病毒检测与防御功能。**(需提供产 品功能截图证明并提供官方检测机构出具关于“勒索病毒”的证书或检测报告证明功能有效性，加盖原厂公章)** 11. 1年租用服务。 |
| 数据库审计 | 1. 提供不限制数据库数量的数据库审计服务，数据库流量（单向）≥400Mb/s，SQL处理性能≥10000条/s。 2. ▲支持与现有云上安全感知平台联动实现数据外发泄密分析**（提供产品功能截图，并加盖原厂公章）** 3. 支持时间段、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索。 4. 支持以时间、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL模版为条件的数据库风险查询。 5. 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 6. 支持自定义策略配置，策略类型支持风险监控、白名单、黑名单，监控级别支持高风险、中风险、低风险 7. 为保障云上数据库安全，要求数据库审计组件内置SQL安全规则，包括导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表等（提供证明截图并加盖原产公章） 8. ▲所投产品的生产厂商入围了第十届CNCERT网络安全应急服务支撑单位名单（甲级）。**（提供证明材料并加盖原厂公章）** 9. 1年租用服务。 |
| Web网站安全防护 | 1. 提供满足业务需求的WEB网站安全防护能力，≥8个web防护授权，HTTP并发连接数≥80000。 2. 支持镜像和容器的方式部署在虚拟环境和云平台中。   （3）▲支持自定义语义引擎白名单功能，包含通过Web应用防护规则、URL参数、IP地址、Webshell上传防护、SQL、XSS、后门扫描的方式排除。**（提供产品功能截图，并加盖原厂公章）**  （4）为保障云上业务防护效果，为所投产品的生产厂商需具备云安全成熟度模型 CS-CMMI5认证。(提供证明材料并加盖投标人公章)←  （5）1年租用服务 |
| SSL证书 | 提供SSL证书（服务端和客户端），且均支持ECC、RSA或SM（国密）三种加密方式。1年租用服务。 |
| 主机安全 | 1. 保护主机数量不少于10个，支持统一管理部署在国产化操作系统和非国产化操作系统的主机安全软件。 2. 采用B/S架构设计，管理控制中心高度集成化，无需额外安装或外接数据库即可实现日志存储和分析展示，无需额外安装或对接升级服务器即可实现文件、特征库的升级和分发。 3. ▲具备勒索病毒专防，支持监控诱饵文件，诱饵文件可被实时监控，当勒索病毒对该文件进行修改或加密操作时进行拦截。**（需提供第三方权威测试机构的产品功能检测报告，至少包含报告首页，对应功能测试页和报告尾页，加盖原厂公章）** 4. 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离。 5. ▲支持windows服务器RDP远程登录保护，可开启RDP远程登录二次认证，以防止黑客对服务器的入侵。还可开启RDP文件加白功能，避免黑客入侵服务器后使用EDR对文件/目录加白，加密这些文档进行勒索。**（提供产品功能截图，并加盖原厂公章）** 6. 具备基于人工智能的检测引擎，支持无特征检测技术，有效应对恶意代码及其变种 7. 支持根据统计周期、终端名称、IP地址，补丁信息和漏洞等级等多维度的入侵检测日志，杀毒扫描日志，微隔离日志，合规检测日志，管理员操作日志，运维日志，联动日志等的日志查询和检测 8. 支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议 9. ▲为保障勒索防护效果，需提供国际权威机构AV-Test 2022年针对勒索专项的满分测试报告或截图。**（提供证明材料并加盖原厂公章）** 10. 1年租用服务 |

## 线路租用

（1）提供互联网线路：100M带宽(一主一备，支持IPV6)，考虑线路冗余及保障网络安全， 1年服务。

（1）提供院内网络线路：可选实体VPN或专线打通医院内网。100Mbps带宽以上，一主一备2条网络专线或其它线路冗余措施，保障网络安全，1年服务。

## 安全服务

|  |  |
| --- | --- |
| **名称** | 技术参数 |
| 安全运营服务 | （1）提供不少于10个资产为期1年的7\*24小时安全托管服务。  （2）本次服务需可复用现有虚拟化态势感知平台和流量检测探针组件。  （3）服务方应使用安全工具对服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险  （4）高危可利用漏洞防护：针对服务范围内资产扫描到的高危可利用漏洞，服务方应当为我院做好每一个高危可利用漏洞的防护工作，包括但不限于为我院提供漏洞修复方案和安全设备防护策略，以及帮助我院配置防护规则。要求招标方可以对服务范围内发现的每一个高危可利用漏洞提供防护规则；  （5）个性化的检测规则定制：为了保证安全监测的准确率和服务质量，服务方应当支持用户自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求（提供服务方服务平台支持为用户自定义配置安全规则的截图）  （6）受影响资产排查与加固：安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。  （7）安全策略检查,服务方安全专家每月对我院的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。服务方云端服务平台应当具备丰富的策略检查工具（要求不少于40种策略检查的工具），支持排查安全设备防护策略配置的合理性。  （8）服务质量监控：服务方需为我院提供服务成果展示门户。  **（9）**▲云端服务平台应当做好严格的安全防护，并严格按照《[信息安全技术—网络安全等级保护基本要求](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E6%8A%80%E6%9C%AF%E2%80%94%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E7%AD%89%E7%BA%A7%E4%BF%9D%E6%8A%A4%E5%9F%BA%E6%9C%AC%E8%A6%81%E6%B1%82/53703710?fromModule=lemma_inlink)》完成等级保护测评工作，服务平台至少通过等级保护三级测评；**（服务方应当提供云端服务平台等级保护三级测评通过证明，提供报告首页、基本信息表、等级测评结论首页，以上内容中必须明确指出该平台用于为用户提供7\*24小时的安全托管服务，加盖原厂公章）**  （10）了保障服务效率和质量，服务方的云端服务平台应当具备一套完善的流程编排引擎，能够为客户灵活编排、定义服务流程，并且定义服务的SLA，将服务过程中的各个关键环节按照一定的顺序和规则进行组织和安排，以达到高效、优质的服务目标  （11）为提升安全运营服务对于高级威胁事件分析效率，云端安全托管服务平台支持GPT机器人入口，可以在使用平台时，随时调起机器人进行提问咨询，输入需要解码的内容提问即可解码（需提供功能截图，加盖厂商公章）  （12）▲所投厂商的远程安全托管服务在21、22年中国区IDC中国远程安全托管服务市场占有率排名前三（**提供证明材料并加盖原厂公章）**  （13）提供1年安全运营的原厂服务，提供原厂关于7\*24小时安全服务以及原厂管家运维的承诺函 |
| 渗透测试 | 1. 保证招标方信息系统正常运行前提下，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试，查找针对应用程序的各种漏洞。帮助采购人理解应用系统当前的安全状况，发现在系统复杂结构中的最脆弱链路并针对安全隐患提出解决办法，切实保证信息系统安全。 2. 采购人授权后，投标人应通过模拟黑客攻击行为通过本地或远程方式对目标对象进行非破坏性的入侵测试。渗透测试应至少包括但不限于以下范围的漏洞：WEB应用系统渗透、主机操作系统渗透、数据库系统渗透；渗透测试内容包括但不限于：身份验证类、会话管理类、访问控制类、输入处理类、信息泄露类、第三方应用类； 3. 渗透测试人员应针对使用不同技术手段，发现不同纬度的漏洞进行验证，并形成记录和报告。 4. 服务次数及范围：3个资产/年，互联网业务系统， 含复测。 5. 交付物：《渗透测试报告》。 |

**五、售后服务要求**

**1、安全服务要求**

投标人应保证业务应用系统的支撑环境，包括但不限于服务器、网络、存储等相关物理环境能满足安全***三级等保***要求，依据招标需求向采购人提供本次项目中所涉及安全服务内容。同时供应商需提供完整、可行的安全防护设计方案。

**2、技术支持与服务要求**

**（1）日常运维服务**

投标人提供专门运维服务团队完成日常运维服务，设立专职人员，由其负责组织和协调采购人处理云平台使用过程中出现的各类问题，包括系统使用、管理、升级和维护。

▲为简化运维管理难度，提高业务上线效率，我院要求本次项目所采购的堡垒机、数据库审计、负载均衡等设备能够与一期云上设备统一管理，并支持配置同步。（需提供证明材料，并加盖投标人公章）

投标人团队在日常安全运维管理中应包括但不限于以下方面工作：1.组织定期评估网络运行安全风险；2.防范计算机病毒和网络攻击、入侵等危害网络安全行为的防护措施；3.监测、记录网络运行状态、网络安全事件的技术手段，做好安全防护；4.做好网络、数据库操作日志，日志留存不少于六个月。

**（2）故障响应服务**

投标人应当提供高效的系统维护服务，有效防范系统风险，需保持7\*24小时电话畅通，能够在系统发生故障问题时，能够协调人力资源在5分钟内响应，30分钟内解决故障。

（**3）重点保障要求**

为保障业务高峰期内系统平稳运行，缓解系统高峰期内因业务发生量增大而带来系统压力风险，要求供应商根据业务周期性特点，加大运维保障力度，保证在业务高峰期内系统平稳运行。对安全厂商、上级部门的漏扫报告及时进行一对一技术分析与处理，并形成书面报告。

**（4）部署迁移服务**

**采购人因业务与安全服务需要涉及到部分项目的迁移，投标人应根据采购人要求完成系统迁移工作，系统中断时间不得超过3小时，迁移过程中产生的所有费用由投标人承担。**

投标人在建设期除了提供安全云服务外，还需要将医院内网映射在互联网的资产统一扎口管理，包括但不限于打卡预约平台、短信平台、支付平台、小程序软件等，以一个二级域名+多个端口+多个路径的模式（举例如http://xxx.aaa.com:80/1/2/3---、https://xxx.aaa.com:443/1/2/3---等）对照映射以上多个业务，支持日志管理记录用户访问、系统运行等完整日志并具备完整性验证功能，协助开通互联网80和443端口并备案；（需要提供完整解决方案和承诺函）

**（5）服务承诺**：1、在协助采购人完成云平台建设、等保2.0测评、IPv6改造等相关实施过程中，采购人将不予额外支出完成项目所需的其它费用，包括人工、运输、安装、辅材及其它一切与本项目相关的衍生费用。（需要提供承诺函）2、投标人须协助医院完成基于网络安全等级保护2.0标准的第三方机构测评，综合得分不低于80分；（需要提供承诺函）3、按照“谁建设、运营，谁负责”、“谁管理、使用，谁负责”的原则落实网络安全工作责任，保障安全防护措施与信息化项目同步规划、同步建设、同步使用。投标人应明确对IPv6互联网业务安全管理平台的运维和安全管理责任。4、采购人在租赁过程中收集、产生、存储的数据和文档属于采购人、采购人有权对这些资源访问、利用支配，承建商须严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏给第三方，未经采购人许可不得访问、修改、披露、转文具、销毁。5、如采购人提前终止某项业务，应在1个月内提前告知投标人，投标人应对停止的业务所涉数据进行安全迁移或可靠的销毁，对账号、地址、域名等及时注销或关闭。（需要提供承诺函）7、发生纠纷时双方应在约定期限内仍能保证采购人数据安全。

**十、评分表（综合评分法）**

|  |  |
| --- | --- |
| **评分项目** | **评分方法** |
| 价格（30分） | 投标单位价格分采用低价优先法计算，即满足招标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。其他投标单位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）×30（四舍五入小数点后保留两位数字） |
| 评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，评标委员会有权要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人如不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。 |
| 技术性能（30分） | 根据采购文件提供的技术参数逐条对比，完全满足采购文件要求得30分；其中打“▲”号为重要指标参数、软件功能及其他要求逐条对比，有一条负偏离每项扣2分，扣完为止；非打 “▲”号指标参数、软件功能及其他要求逐条对比，有一条负偏离每项扣1分，扣完为止。 |
| 技术方案（13分） | 1、投标人需充分理解采购人对本项目的整体要求，提供项目整体技术方案，包括系统架构、技术路线、安全保障、扩展性强，方案能突出数据安全（云资源位置、安全组件配置等）、系统访问性能（线路带宽、并发数、延时性等）、设备统一管理等内容。（5分） |
| （1）技术方案内容清晰、严密、合理，资源扩展性强且支持设备统一管理，得5分； |
| （2）技术内容较为清晰、严密、合理，资源扩展性一般，不支持设备统一管理，得3分； |
| （3）技术内容欠清晰、合理，资源扩展性差，不支持设备统一管理，得1分； |
| （4）不提供不得分。 |
| 2、投标人需提供针对本项目的实施与培训方案，包括项目人员计划、项目组织计划、质量保障、业务迁移部署、统一扎口管理、培训内容等。（5分） |
| （1）方案科学、合理，可操作性强，得5分； |
| （2）方案较科学、合理，具有一定的可操作性，得3分； |
| （3）方案基本合理，基本可操作，得1分； |
| （4）不提供不得分。 |
| 3、投标人需提供针对本项目的安全建设方案，包括安全产品质量性、运行稳定性、无单点故障安全隐患等。（3分） |
| （1）方案科学、合理，可操作性强，得3分； |
| （2）方案较科学、合理，具有一定的可操作性，得2分； |
| （3）方案基本合理，基本可操作，得1分； |
| （4）不提供不得分。 |
| 综合实力（17分） | 1、投标人具有信息系统服务交付能力等级(CCID)证书认证证书，一级得3分，二级及以下的得1分，没有不得分，本项满分3分。 |
| 2、投标人具有大数据服务安全能力评价认证证书，得3分，不提供不得分。本项满分3分。 |
| 3. 投标人具有信息技术服务管理体系认证、云服务信息安全管理体系认证证书，每提供一个证书得0.5分，满分1分 |
| **（以上证书需提供复印件加盖并投标人公章）** |
| 1、为保证平台可靠性与安全性，云技术提供厂商具备CSA-CMMI5证书。 |
| 2、云技术提供厂商需具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质（一级） |
| 3、云计算提供厂商需要是《信息技术云计算平台即服务部署要求》（GB/T 37739-2019）起草单位之一。 |
| 每符合一项得2分，全部符合得6分，不符合不得分。**（注：1-3项须提供相关证明材料，并加盖厂家公章）** |
| 1、项目负责人需要具备系统分析师、信息系统项目管理师、网络工程师证书，每提供一个证书得 0.5分，满分1.5分； |
| 2、服务团队成员需具有注册信息安全专业人员CISP证书、网络规划设计师证书、数据库系统工程师证书、高级IT运维工程师证书、公有云能力认证资格证书，每提供一个证书得0.5分，满分2.5分。 |
| 3、**（以上人员需提供证书及投标人为相关人员缴纳的近三个月的社保证明复印件并加盖投标人公章）** |
| 业绩（5分） | 供应商提供 2021年1月1日至今(以合同签订目期为准)，与本项目类似的业绩，每提供一份合同得1分，满分5分。(须提供合同，原件扫描上传) |
| 售后运维服务（5分） | 1、 投标人需提供本项目详细的运维服务及应急响应方案，包含但不限于运维团队、运维计划、定期巡检、突发状况的调度安排、应急处理等。（5分） |
| （1）运维方案合理、可操作性强，应急处理及时，优于采购要求,得5分； |
| （2）运维方案一般,应急处理基本满足采购要求,得2分； |
| （3）运维方案存在运维操作风险、应急处理未能全部满足项目要求，得1分； |
| （4）不提供不得分。 |

**三、投标人须知**

**（一）编制要求**

1、投标人应在仔细阅读院内公开谈判文件的基础上，按招标方要求认真编写投标文件，并加盖投标单位公章。投标人提供的投标文件必须真实、详尽。所有投标文件须有总目录和总页码，每份标书从起始页依次插入连续的页码。投标文件袋须密封良好并加盖骑缝印章，送达指定地点，逾时送交的材料概不接受。

2、投标人在收到院内公开谈判文件后，若有疑问应以书面形式（包括书面文字、传真、电子邮件等）在规定时间前向招标人提出。招标人将所有问题集中后在统一答复所有投标人。

3、明确标明“正本”或“副本”字样，一旦正本和副本有差异，以正本为准。所有投标资料均需A4纸打印，按照院内公开谈判文件规定的顺序装订。

**（二）资格审查要求**

**1、资格审查方式为资格后审。投标截止时间(2024年6月17日17：00)前须向招标人提供书面法人授权委托书，该授权委托代理为该项目指定联系人。**

投标人资质要求

1 投标人要求

投标人必须是具有独立法人资格的公司。

2 承担本项目能力和资格的有关资格证明材料

1) 由工商局签发的投标人工商营业执照副本复印件（加盖公章）；

2) 投标人各类资质证书材料复印件（加盖公章）

3) 服务能力：投标方必须具备实施项目开展和提供后续服务的能力，需提供人员及服务承诺（格式自拟）。

4) 近三年以来完成相关项目一览表；

**（三）投标文件要求**

1、**投标文件的组成**：

1.1资格审查文件，所有复印件需加盖公章：

（1）针对本项目院内公开谈判的授权委托书；

1. 企业法人营业执照；
2. 企业资质证书；

**1.2报价文件**

（1）投标函

（2）授权委托书

（3）投标报价

**（四）开标、评标**

1、开标时，招标方代表或监管部门或投标单位检查投标文件的密封情况，在确认无误后拆封读标。投标文件一经开封不得进行改动。

2、初步评审要求：开标后，招标方将组织审查投标文件是否完整；是否有计算错误。投标文件出现下列情形之一的，将作为无效投标文件：

（1）投标文件不响应院内公开谈判文件要求的；

（2）投标函未盖投标人的企业及企业法定代表人印章并签字的，或者企业法定代表人委托代理人没有合法、有效的委托书（原件）及委托代理人印章并签字的；

（3）投标文件的关键内容模糊、无法辨认的；

3、评标小组先评审技术文件，后评审报价文件。

4、严格按照扬州大学采购管理暂行办法，组成项目评标小组。严格按招标文件，公平、公正、科学、严谨地对投标文件进行综合评定。

5、院内公开谈判程序：

**（1）资格审查；（2）需求响应评审；（3）价格谈判，二次报价。**

6、定标

综合评分第一的单位为中标单位。

**四、投标文件格式及附件要求**

**目录**

（一）资格审查

1、针对本项目的授权委托书原件；

2、企业法人营业执照；

3、企业资质证书；

4、由社保部门出具的投标人为经办人及投标报名项目负责人缴纳的近三个月中任意一个月养老保险费用的证明材料（任意一个月）；

5、投标单位不在供应商被“信用中国”网站（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的截图，并盖章。

（二）报价文件

1、投标函

2、授权委托书

3、投标报价

4、供应商廉洁自律承诺书

（三）其他（格式自拟）

**授权委书**

本授权委托书声明：我(姓名) 系(投标人名称) 的法定代表人，现授权委托我单位的(姓名) 为我公司代理人。代理人在 项目院内公开谈判活动中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

代理人无转委权。特此委托。

投标人：(盖章)

法定代表人：(签字)

日期： 年 月 日

代理人姓名：签字：

身份证复印件：

承诺书(一)

致：扬州大学附属医院（招标人名称）

我公司自愿参加贵单位项目的院内公开谈判，并接受对我公司的资格审查，我公司承诺：根据贵单位提出的资格审查合格条件标准和要求，本公司没有因骗取中标或者严重违约以及发生重大质量、安全生产事故等问题，被有关部门暂停投标资格并在暂停期内。

本公司递交的资格审查申请书中的内容没有隐瞒、虚假、伪造等弄虚作假行为。

单位：（公章）

法定代表人签字：

项目负责人签名：

年 月 日

**投标函**

招标人： 扬州大学附属医院

根据已收到贵方的项目的院内公开谈判文件，遵照扬州大学附属医院采购管理办法，我单位经研究上述院内公开谈判文件的投标须知、合同条件、技术规范、和其他有关文件后，我方投标报价为

万元。

代理服务费收取费率：

投标人（盖章）：

法定代表人或授权委托人（签字）：

日 期：

**投标报价**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目内容** | **投标内容** | **报价** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | 其他条件 |  | |

投标人（盖章）：

法定代表人或委托代理人（签字）：

日 期：

**供应商廉洁自律承诺书**

扬州大学附属医院 院内公开谈判是实行公开、公平、公正的阳光工程，给予了每个供应商平等竞争的机会。作为参与此次院内公开谈判活动的承包商,我公司现郑重作出以下承诺：

一、遵守《中华人民共和国政府采购法》及省、市有关政府采购的各项法律、法规和制度以及《扬州大学附属医院采购管理暂行办法》的规定。

二、客观真实反映自身情况，按规定接受采购供应商资格审查,不提供虚假材料，不夸大自身技术和提供服务的能力。

三、以合法正当的手段参与采购的公平竞争。不与采购人、其他供应商或者采购代理机构恶意串通，不以不正当手段诋毁、排挤其他供应商，不向采购人、评审机构行贿或者提供其他不正当利益。

四、在采购活动中，认真履行规定义务,包括:遵守采购程序，按要求编写投标、响应文件，并保证投标、响应文件内容的真实可靠；按时递交投标、响应文件；在评标、谈判现场遵守相关纪律，不影响正常的采购秩序。

五、自觉接受采购监督管理部门及其他相关部门的监督检查。

**如违反以上承诺，我公司愿承担一切法律责任，并接受采购监督管理部门及其他相关部门依法作出的处罚。**

承诺单位（盖章）

法定代表人（授权代表签字）：

2024年 月 日