网络安全加固及商用密码安全性改造项目需求

网络安全加固及商用密码安全性改造项目——以增强院区网络安全建设，拟于2025年4月启动招标采购，预算金额110万元。

为制定更加全面、科学、满足医院实际需要的采购需求，并做好招标控制价的核定，现面向社会开展市场调研工作。

本项目需满足的基本需求包括：

（一）项目内容（详见技术参数）

通过分析我院当前信息化安全现状，并结合我院信息化建设规划，在充分调研的基础上，从技术+服务方向进行着手。技术方面围绕病毒防护，外网防护能力的补充，国密认证能力补充,国内最权威威胁情报联防阻断能力，全生命周期的数据安全风险防护等方向进行全方位的安全建设，要与现有安全保障体系充分融合。

（二）服务要求

1、服务方面提供三年原厂现场技术支持，包括但不限于：渗透测试、风险评估、安全保障、应急响应，培训、基线核查、配合软件厂商整改恢复业务系统。软件维保3年、硬件维保3年。质保服务期从合同签订之日开始；

2、需提供项目实施方案，内容包括但不限于：实施人员名单（姓名，联系方式等）、项目实施计划等；

3、需提供项目售后服务方案，内容包括但不限于：售后负责人员名单（姓名，联系方式等）、项目售后服务内容等。

（三）技术参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **货物名称** |  | **单位** | **数量** |
| 1 | 防病毒网关 | 千兆电口≥8个（Bypass电口≥6）；防病毒吞吐率≥2Gbps；电源：双冗余电源；扩展插槽≥2；硬盘≥1T  ，针对Windows和Linux下的挖矿、勒索、木马、蠕虫、灰色软件等病毒进行精准查杀；持续优化高性能扫描引擎和网络威胁检测引擎，有效阻止挖矿攻击及其他网络事件入侵、漏洞利用攻击、APT攻击、C&C外联等恶意行为，能够针对1DAY、NDAY漏洞进行快速响应，有效保护用户网络内部的数据资产安全。 | 台 | 1 |
| 2 | 防火墙 | 针对外网系统做定向安全防护。网络层吞吐量：≥20G，应用层吞吐量：≥10G，防病毒吞吐量：≥1.5G，IPS吞吐量：≥1.5G，全威胁吞吐量：≥1G，并发连接数：≥300万，HTTP新建连接数：≥9万，硬件参数：内存大小：≥8G，硬盘容量：≥128G SSD，接口：≥8千兆电口+≥2万兆光口SFP+，≥8个千兆光。 | 台 | 1 |
| 3 | 威胁情报联防阻断服务 | 依托权威机构业界顶尖的安全情报源，对互联网恶意攻击、被控外联等行为进行实时研判、预警和威胁拦截，实现“一点监测、全网阻断、精准防护、联防联控”的防护效果。 | 年 | 1 |
| 4 | 零信任系统 | 最大理论加密流量（Mbps）：≥600，最大理论建议并发用户数：≥1200，最大理论https并发连接数（个）：≥60000，理论https新建连接数（个/秒）：≥240；性能参数：加密最大流量（Mbps）：≥170，理论并发隧道数（Tunnel）：≥600。硬件参数：规格：≥1U，内存大小：≥16G，硬盘容量：≥128G SSD，电源：冗余电源，接口：≥6千兆电口+≥4千兆光口SFP；≥500零信任接入授权（授权买断）并发;≥200套移动版授权（授权买断）;3年\* 软件升级;3年\* 产品质保（标准版）;3年移动应用自动封装服务。 | 台 | 1 |
| 5 | 网络防泄漏 | 内存≥64G;接口：千兆电口≥6个，1\*IPMI，6\*USB3.0+1\*VGA+1\*串口;硬盘≥2T；电源：冗余电源;可扩展槽位≥3。  1） 梳理外网敏感数据，并对外网数据外发进行管控，防止敏感数据泄露。  2） 对全流量通道进行监控，实现全通道的外发内容监控。包括对Web应用监控、邮件监控、文件传输监控等互联网通道的传输监控。  3） 对敏感内容进行多元化的处置措施，实现精细化的管控，提供包括审计放行、邮件告警、文件留存、备注放行等处置措施。 | 台 | 1 |
| 6 | 数据库访问控制系统 | 内存≥32G；硬盘≥4T；千兆电口≥6，扩展插槽≥2个；USB 3.0≥4个，1个Console口，1个VGA/HDMI口，冗余电源；授权≥32个数据库示例。  1）对数据库中表、字段进行精细化管控。  2）针对运维过程中账号管理混乱、运维操作不透明等一系列不合规现象造成的数据泄漏事件，实现操作定位到人、责任到人的目的，帮助实现运维人员的身份统一管理、运维合规。  3）实现运维人员、外包开发人员根据其工作所需和安全等级访问敏感数据，并对核心生产库的重要敏感数据进行动态脱敏。 | 台 | 1 |
| 7 | 云WAF | 提供云端Web应用安全防护、入侵防护、实时攻击监测、防扫描、CC攻击防护、一键关停、永久在线、手机APP运维、安全防护报告、安全可视，至少授权1个一级域名，10个二级域名 | 年 | 1 |
| 8 | 安全服务 | 1）系统渗透测试：针对测评机构未测出的重大漏洞及弱口令进行安全渗透测试服务，发现相关漏洞和弱口令。  2）其他安全应急保障：针对公安等监管部门通报的网络中突发网络安全事件进行应急保障，配合溯源，保障安全事件快速修复和上线 | 年 | 1 |