龙岩市第三医院网络安全运维服务及安全设备续保项目

市场调研公告

根据我院业务发展需要，拟对福建省龙岩市第三医院网络安全运维服务及安全设备续保项目市场调研公告，欢迎符合条件的相关厂商或供应商参与。

**一、资质要求**

1.具备《中华人民共和国政府采购法》第二十二条规定的条件。

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（六）法律、行政法规规定的其他条件。

2.具有本次招标项目的生产或经营范围，有能力提供本次招标项目及所要求的服务。

3．本项目不接受联合体或代理方式参与，只允许参与人自己履行该项服务。参与人亦不得借用母公司、子公司或控股公司的资质参与本项目参与，参与人如有更名，需提供相关证明文件。

**二、市场调研项目**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目** | **数量** | **单位** | **服务期限** | **限价（元/年）** |
| 1 | 网络安全运维服务 | 1 | 年 | 1年 | 人民币：200000 元/年 |
| 2 | 安全设备续保 | 1 | 批 | 3年 | 人民币：150000 元/年 |

相关参数要求：

**1、网络安全运维服务**

1.1 服务目标

根据信息系统安全等级保护相关法规和标准要求，对龙岩第三医院信息系统安全进行全风险评估，通过每季度的信息系统安全巡查，发现当前网络及信息系统存在的各种安全风险，提出解决方法并协助对问题进行整改加固。同时，通过安排专业服务人员和提供定期的安全巡检、渗透测试、安全加固，实行7\*24小时原厂技术服务，对突发事件进行应急响应，并提供定时通告与防护等服务。确保信息系统在日常运行过程中得到专业化的安全保障，能够应对当前以及未来一段时间的安全威胁，保障重要业务安全可靠的运行。

1.2 服务范围

本次安全运维服务的主要对象是与医院信息化业务相关的所有软硬件资产。

1.3 项目期限

服务期限为一年。

1.4 服务内容

定期提供的安全咨询服务、安全风险评估、安全巡检、渗透性测试、漏洞扫描、安全加固、重保服务、应急保障、管理制度辅助建设、人员技能培训和其他支持等服务。

序号1：安全运维服务清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务项目** | **服务内容** | **服务范围** | **服务频度** | **交付成果** |
| 1 | 安全咨询 | 网络边界及安全域分析、网络拓扑重现、现有安全措施分析、网络安全规划设计（3-5年） | 医院网络 | 全年 | 《网络安全规划设计》 |
| 2 | 风险评估 | 网络架构安全风险评估、网络设备风险评估、安全设备风险评估、主机[服务器](https://www.fastadmin.net/go/aliyun)系统安全风险评估、核心业务系统安全风险评估、客户端抽样安全风险评估。 | 医院网络 | 每年1次 | 《网络信息系统安全风险评估报告》 |
| 3 | 安全巡检 | 硬件措施有效性及策略核查（防火墙、入侵检测等）、软件措施有效性及策略核查（防篡改、防病毒、终端管理等）以及医院资产（主机、服务器、网络设备、操作系统、数据库、应用系统等）进行安全巡检。 | 医院资产 | 每年4次 | 《网络安全巡检报告》 |
| 4 | 渗透测试 | 对核心业务系统定期进行人工渗透测试 | 医院系统 | 每年2次 | 《渗透测试报告》 |
| 5 | 漏洞扫描 | 对医院核心资产（主机、服务器、网络设备、操作系统、数据库、应用系统等）进行定期漏洞扫描 | 医院资产 | 每年4次 | 《漏洞扫描报告》 |
| 6 | 安全加固 | 1.对医院核心[服务器](https://www.fastadmin.net/go/aliyun)系统进行安全加固2.业务系统安全加固辅导3.安全设备进行加固4.网络安全策略进行加固 | 医院资产 | 每发现漏洞后 | 《安全加固实施方案》 |
| 7 | 重保服务 | 1.提供重要时期以及攻防演习期间的网络安全保障工作支持服务，必要时派人驻场服务。2.当网络或系统出现安全事件时，需提供安全应急专家进行现场安全应急响应工作。 | 医院网络 | 重要时期、攻防演练期间 | 《重保服务报告》或《攻防演练报告》 |
| 8 | 应急保障 | 当网络或系统出现安全事件时，须在30分钟内提供解决方案。对于可以远程解决的事件，必须在30分钟内指派专业工程师对接，对于必须到达现场解决的事件，工作日2小时，非工作日4小时内到达现场。到达现场后24小时内解决事件，恢复网络与信息系统。在网络与信息系统恢复正常后，应在一周之内提供完整的安全事件分析处理报告。 | 医院内部 | 全年 | 《应急处理报告》 |
| 9 | 培训服务 | 提供面向信息技术人员定制化安全培训。 | 现场 | 2个名额 | 培训通知等 |
| 10 | 制度建设 | 辅助福建省龙岩市第三医院建设安全管理制度 | 院内网信管理制度 | 全年 | 相关网信管理制度文档 |
| 11 | 其他支持 | 提供网络安全宣传素材，配合上级单位、网信办、网安等外部检查单位的安全检查工作，每项服务完成后5个工作日内提供相关服务报告。 | 医院内部 | 全年 | 《网络安全宣传活动素材》《安全服务报告》 |

**2.安全设备续保**

序号2：安全产品续保服务清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **型号** | **数量** | **服务期限** |
| 1 | 数据中心防火墙 | 品牌：天融信 型号：NGFW4000 | 1 | 提供3年原厂续保服务 |
| 2 | 网络准入控制 | 品牌：天融信 型号：TopNAC | 1 |
| 3 | 终端管理系统 | 品牌：天融信 型号：TSM | 1 |
| 4 | 数据库审计 | 品牌：天融信 型号：TopAudit | 1 |
| 5 | WEB应用防护抗攻击系统 | 品牌：天融信 型号：TopWAF | 1 |
| 6 | 上网行为管理 | 品牌：天融信 型号：TopACM | 1 |
| 7 | 运维区防火墙 | 品牌：天融信 型号：NGFW4000 | 1 |
| 8 | 防病毒软件 | 品牌：天融信 型号：TopEDR | 1 |
| 9 | 入侵防御 | 数据中心防火墙开启此项功能 | 1 |

提供以上安全设备原厂3年续保、软件（含杀毒软件等的病毒库、特征库）等升级,**并提供原厂授权函。**

**三、**技术要求

1.参与人应具备足够的医疗行业信息安全服务类实施经验，应至少具备一家三级医院信息安全服务类项目实施经验（须提供有效合同复印件证明）。

2..参与人应具备中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类三级）（须提供证书复印件）。

3.参与人应具备国家互联网应急中心颁发的网络安全应急服务支撑单位证书（须提供证书复印件）。

四、调研文件要求

请按以下顺序装订材料，每页加盖公章。

1.营业执照复印件

2.法定代表人授权委托书

3.法定代表人、被授权人身份证复印件

**4.续保产品服务原厂授权函（盖原厂公章）**

5.安全运维方案（不能低于服务清单内容）。

6.三级医院信息安全服务类项目实施经验（须提供有效合同复印件证明）

7.中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类三级）

8.国家互联网应急中心颁发的网络安全应急服务支撑单位证书

以上所有材料均加盖公章装订成册，并于封面注明项目名称、单位名称、联系人、联系方式（固定电话及手机号码），加盖公章。

五、文件截止递交时间

1.文件递交截止时间:2023年9月12日18时（周末及法定节假日除外）。

2.文件递交地址：龙岩市第三医院信息科（门诊4楼）（可邮寄）

3.联系人： 袁先生      联系电话： 0597-3291212

4.公示日期：2023年９月６日-2023年９月1２日

5.我院将择期召开市场调研会，时间另行通知。届时，需携带所投项目报价表（附件1）和项目具体内容各６份，加盖公章并用信封密封，现场拆封。

＊特别声明：本工作仅为对拟采购项目进行市场调研，对参与报名的供应商不作任何承诺，不承诺和最终采购绝对相关联。

附件1：

**报价表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目** | **数量** | **单位** | **期限** | **报价（元/年）** |
| 1 | 网络安全运维服务 | 1 | 年 | 1年 | 人民币： 元/年 |
| 2 | 安全设备续保 | 1 | 批 | 3年 | 人民币： 元/年 |