**贵州航天医院2023年网络与信息安全等级保护测评项目**

**附件一 采购需求**

1. 测评要求：

|  |  |  |
| --- | --- | --- |
| **序号** | **项目** | **要求** |
| 1 | HIS三级等保测评 | 1. 按等保要求对我单位医院信息系统（HIS）开展三级等保测评工作。 2. 从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个方面，对被测评对象进行综合测评。 |
| 2 | 定期安全巡检 | 1. 每半年开展一次巡检工作。 2. 巡检范围包括门户网站、LIS系统、PACS系统、OA业务系统、HIS系统等，涉及机房的所有服务器、核心网络设备、安全设备。（若整改过程新增安全设备，在服务期内进行安全巡检工作）。 3. 漏洞扫描、渗透测试涉及门户网站、LIS系统、PACS系统、OA业务系统、HIS系统等和相关服务器、数据库。 4. 提交《资产台账表》和《漏洞台账表》，每季度进行更新。 5. 每半年出具《网络安全巡检报告》。 |
| 3 | 全网风险评估服务 | 1. 通过梳理、资产识别，建立信息系统、IT设施台账，梳理信息资产责任人、详细记录设备部署、服务配置等内容。（资产台账在定期巡检过程每季度更新） 2. 针对所有信息系统，采取漏洞扫描、渗透测试、安全基线配置核查和病毒木马专项检查等方式，全面评估网络安全的工作，识别、分析威胁、脆弱性，形成风险评估报告。 3. 评估范围包括门户网站、LIS系统、PACS系统、OA业务系统、HIS系统等，涉及机房的所有服务器、核心网络设备、安全设备等信息资产。 4. 业务系统相关服务器、网络设备、安全设备等信息资产的型号、登录方式及密码、管理人员、物理位置等资产识别梳理。 5. 按照国家标准风险评估规范、网络安全等级保护测评等相关要求进行基线检查。 |
| 4 | 网络安全教育意识培训 | 提供网络安全技术专题培训，培训主题包括但不限于：等保测评2.0解读、网络安全意识、政策、网络知识、日常安全防护、应急处置、密码应用以及网络安全管理运维等。 |
| 5 | 应急演练 | 1. 协助修订整体应急预案以及不同场景应急预案。 2. 每个系统可提供多种场景以上故障事件场景进行应急演练操作；根据应急预案制度应急演练方案，明确演练参与人员、工作职责及演练范围和故障事件场景；配合虚拟演练场景搭建；根据演练方案开展现场应急演练；出具应急演练报告。 |
| 6 | 应急响应 | 1. 提供现场及远程（非紧急时）技术支撑。 2. 对上级部门网络安全预警进行排查。 3. 提供应急处置报告。 |

1. 评分办法：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评分项目** | **标准分** | **评分标准** |
| 1 | 投标报价 | 20 | 经评审合格的各投标人投标价的算术平均价为基准价，超出采购人预算价或低于项目预算价格50%的报价为无效报价，不作为评标基准价；  投标人的有效投标价等于评标基准价时，其报价分为满分20分；四舍五入保留两位小数，每高于基准价一个百分点扣1分，每低于基准价一个百分点扣0.5分，扣完为止；  如投标人报价为无效报价，其报价得分为零分；  如投标人的报价均为无效报价，且采购人不能接受的将重新招标。 |
| 2 | 技术方案 | 30 | 1. 第一档次（16-20分）：服务方案整体编制科学合理、重点突出，针对性强，完全满足采购人实际需求，测评服务方案、售后服务方案、风险把控、保密措施具体完整。 2. 第二档次（11-15分）：服务方案整体编制合理，有侧重点，有一定针对性，基本满足采购人实际需求；测评服务方案、售后服务方案、风险把控、保密措施合理。 3. 第三档次（6-10分）：服务方案整体编制基本合理，有侧重点，有一定针对性，基本满足采购人实际需求；测评服务方案、售后服务方案、风险把控、保密措施基本合理。 4. 第四档次（0-5分）：服务方案编制粗糙、杂乱、未突出重点，针对性差，无法满足采购人实际需求； 5. 投标人服务期间所选用的安全工具中包含：    1. 包含有漏洞扫描工具，得2分；    2. 包含WEB 应用扫描工具，得2分；    3. 包含数据库核查工具，得2分；    4. 包含网络检查工具，得2分；    5. 包含恶意代码检查工具，得2分。   （以上工具可以是自主开发、采购第三方工具，自主开发需要提供软件著作等证明材料，第三方工具需要提供采购合同。） |
| 3 | 供应商资质 | 30 | 1. 具备网络安全等级测评与检测评估机构服务认证证书，并在“中国网络安全等级保护网”全国网络安全等级测评与检测评估机构目录中，且近五年未被行业主管部门处罚、暂停业务等，得5分； 2. 具有中国合格评定国家认可委员会颁发的检验机构认可证书CNAS得4分； 3. 投标人在《商用密码应用安全性评估试点机构目录》（国家密码管理 局第42号公告）中，得4分； 4. 具备检验检测机构-资质认定证书（CMA）证书，得4分； 5. 具备中国通信企业协会颁发的网络安全服务能力评定证书（应急响应类及网络安全培训类）,得4分； 6. 具有工业信息安全测试评估机构证书，得4分； 7. 具备有效的知识产权管理体系认证证书（认证范围包括等保测评T29490-2013）得5分； |
| 4 | 服务保障 | 20 | 1. 项目经理    1. 项目经理具备高级等保测评师证书，得3分；    2. 具备注册信息安全专业人员(CISP)证书、国家重要信息系统保护人员、注册网络安全测评专业人员(NSATP)证书，缺一不可，得3分； 2. 项目成员(不含项目经理)    1. 项目成员具有1名及以上高级测评师，得3分；具有2名及以上中级测评师，得3分；具有2名及以上初级测评师，得2分；    2. 项目成员具有1名及以上注册网络安全渗透评估专业人员（NSATP-A），得3分；    3. 项目成员具有1名及以上注册网络安全专业防御人员（NSATP-D），得3分。   （以上人员不能重复，须提供资质证明、职称证书以及供应商所在地社保机构出具的由供应商为以上人员缴纳的社保证明，社保证明需加盖社保机构公章，否则不予计分。） |