采购清单及相关要求

**第一节 采购内容及服务要求**

1、项目概况

为深入贯彻落实习近平总书记关于网络安全工作的重要指示精神和《网络安全法》要求，根据公安部、国信办联合印发《信息系统安全等级保护管理办法》（公通字【2007】43号）、《关于信息系统安全等级保护工作的实施意见》（公通字【2004】66号）、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安【2007】861号）等相关文件要求，我单位拟对以下本单位信息系统开展网络安全等级保护测评工作：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **测评系统名称** | **定级情况** | **简要说明** |
| 1 | 马鞍山市区域卫生信息平台 | 三级 | 信息安全等级保护测评 |

2、技术要求

**(一).测评依据**

《信息安全技术信息系统安全等级保护基本要求》GB/T 22239-2008

《信息安全技术信息系统安全等级保护测评要求》GB/T 28448-2012

《信息安全技术信息系统安全等级保护测评过程指南》GB/T 28449-2012

**(二).测评原则**

（1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标人的行为，否则招标人有权追究投标人的责任。

（2）标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

（3）规范性原则：投标人的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

（4）可控性原则：测评服务的进度要跟上进度表的安排，保证招标人对于测评工作的可控性。

（5）整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

（6）最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响。

**(三).单元测评**

**（1）物理安全**

物理安全测评将通过访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况。在内容上，物理安全层面测评实施过程涉及10个测评单元。

各个测评指标的具体内容和测评要求见表3.1。

表3.1 物理安全测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 物理位置的选择 | 通过访谈物理安全负责人，检查主机房等过程，测评主机房等信息系统物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。 |
| 2 | 物理访问控制 | 通过访谈物理安全负责人，检查主机房出入口、机房分区域情况等过程，测评信息系统在物理访问控制方面的安全防范能力。 |
| 3 | 防盗窃和防破坏 | 通过访谈物理安全负责人，检查主机房主要设备、介质和防盗报警系统等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。 |
| 4 | 防雷击 | 通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。 |
| 5 | 防火 | 通过访谈物理安全责任人，检查机房设计/验收文档，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。 |
| 6 | 防水和防潮 | 通过访谈物理安全负责人，检查主机房和除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。 |
| 7 | 防静电 | 通过访谈物理安全负责人，检查主机房等过程，测评信息系统是否采取必要措施防止静电的产生。 |
| 8 | 温湿度控制 | 通过访谈物理安全负责人，检查主机房恒温恒湿系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。 |
| 9 | 电力供应 | 通过访谈物理安全负责人，检查主机房供电线路、设备等过程，测评信息系统是否具备提供一定的电力供应的能力。 |
| 10 | 电磁防护 | 通过访谈物理安全责任人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。 |

**（2）网络安全**

网络安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的网络安全保障情况。在内容上，网络安全层面测评实施过程涉及7个测评单元。

各个测评指标的具体内容和测评要求见表3.2。

表3.2 网络安全测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 结构安全 | 通过访谈网络管理员，检查网络拓扑情况、抽查核心交换机、接入交换机和接入路由器等网络互联设备，测试系统访问路径和网络带宽分配情况等过程，测评分析网络架构与网段划分、隔离等情况的合理性和有效性。 |
| 2 | 访问控制 | 通过访谈安全员，检查防火墙等网络访问控制设备，测试系统对外暴露安全漏洞情况等过程，测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。 |
| 3 | 安全审计 | 通过访谈审计员，检查核心交换机和接入交换机等网络互联设备的安全审计情况等，测评分析信息系统审计配置和审计记录保护情况。 |
| 4 | 边界完整性检查 | 通过访谈安全员，检查边界完整性检查设备，接入边界完整性检查设备进行测试等过程，测评分析信息系统私自联到外部网络的行为。 |
| 5 | 入侵防范 | 通过访谈安全员，检查网络边界处的入侵检查设备IDS/IPS等过程，测评分析信息系统对攻击行为的识别和处理情况。 |
| 6 | 恶意代码防护 | 查看系统在网络边界及核心业务网段处是否有对恶意代码采取相关措施，查看代码库是否更新，询问更新策略。 |
| 7 | 网络设备防护 | 通过访谈网络管理员，检查核心交换机，接入交换机和接入路由器等网络互联设备；IDS和防火墙等网络安全设备，查看它们的安全配置情况，包括身份鉴别、权限分离、登录失败处理、限制非法登陆和登陆连接超时等，考察网络设备自身的安全防范情况。 |

**（3）主机安全**

主机系统安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的主机安全保障情况。在内容上，主机系统安全层面测评实施过程涉及7个测评单元。

各个测评指标的具体内容和测评要求见表3.3。

表3.3 主机安全测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 身份鉴别 | 检查各主机服务器和终端设备相应操作系统或数据库的身份标识与鉴别和用户登录的配置情况。 |
| 2 | 访问控制 | 检查各主机服务器和终端设备相应操作系统或数据库的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。 |
| 3 | 安全审计 | 检查各主机服务器和终端设备相应操作系统或数据库的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。 |
| 4 | 剩余信息保护 | 检查各主机服务器相应操作系统的剩余信息保护情况，查询有关维护手册和操作手册，查看文件、目录和数据库记录等资源所在的存储空间被释放或重新分配前的处理情况。 |
| 5 | 入侵防范 | 检查各主机服务器和终端设备相应操作系统的自我监控能力；检查操作系统对入侵的防范情况。 |
| 6 | 恶意代码防范 | 检查各主机服务器和终端设备相应操作系统的恶意代码防范情况。 |
| 7 | 资源控制 | 检查各主机服务器和终端设备相应操作系统或数据库的系统资源控制情况，如会话限定、用户登录限制、最大并发连接以及服务优先级设置等。 |

**（4） 应用安全**

应用安全测评将通过访谈、配置检查和工具测试的方式测评信息系统的应用安全保障情况。在内容上，应用安全层面测评实施过程涉及7个测评单元。

各个测评指标的具体内容和测评要求见表3.4。

表3.4 应用安全测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 身份鉴别 | 检查业务应用系统的身份标识与鉴别功能设置和使用配置情况；检查业务应用系统对用户登录各种情况的处理，如登录失败处理、登录连接超时等。 |
| 2 | 访问控制 | 检查业务应用系统的访问控制功能设置情况，如访问控制的策略、访问控制粒度、权限设置情况等。 |
| 3 | 安全审计 | 检查业务应用系统的安全审计配置情况，如覆盖范围、记录的项目和内容等；  检查业务应用系统安全审计进程和记录的保护情况。 |
| 4 | 剩余信息保护 | 查看应用系统设计、验收文档，是否采取措施保证对存储介质中的用户鉴别信息进行及时清除。 |
| 5 | 通信完整性 | 检查业务应用系统客户端和服务器端之间的通信完整性保护情况。 |
| 6 | 通信保密性 | 利用协议分析仪检查业务应用系统客户端和服务器端之间的通信保密性保护情况。 |
| 7 | 抗抵赖 | 询问管理员，应用系统是否采取抗抵赖措施，具体措施有哪些。 |
| 8 | 软件容错 | 检查业务应用系统的软件容错能力，如输入输出格式检查、自我状态监控、自我保护、回退等能力。 |
| 9 | 资源控制 | 检查业务应用系统的资源控制情况，如会话限定、用户登录限制、最大并发连接以及服务优先级设置等。 |

**（5）数据安全及备份恢复**

数据安全测评将通过访谈、配置检查的方式测评信息系统的数据安全保障情况。在内容上，数据安全层面测评实施过程涉及3个测评单元。

各个测评指标的具体内容和测评要求见表3.5。

表3.5 数据安全及备份恢复测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 数据完整性 | 检查信息系统的数据完整性保护情况，包括传输完整性、存储完整性保护措施等； |
| 2 | 数据保密性 | 检查信息系统的数据保密性保护情况，包括传输保密性和存储保密性保护措施等。 |
| 3 | 备份和恢复 | 数据的备份情况，包括软、硬件方面的支持情况等。 |

**（6）安全管理制度**

测评对象主要为安全主管人员，安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等，涉及工作单元3个。

各个测评指标的具体内容、测评对象和测评要求见表3.6。

表3.6 安全管理制度测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 管理制度 | 通过访谈安全主管，检查有关管理制度体系文档等过程，测评管理制度体系在内容覆盖上是否全面、完善。 |
| 2 | 制定和发布 | 通过访谈安全主管，检查有关制度制定要求文档等过程，测评管理制度的制定和发布过程是否遵循一定的流程。 |
| 3 | 评审和修订 | 通过访谈安全主管，检查管理制度评审记录等过程，测评管理制度定期评审和修订情况。 |

**（7）安全管理机构**

测评对象主要为安全主管人员、安全管理人员、相关的文件资料和工作记录等，涉及工作单元5个。

各个测评指标的具体内容和测评要求见表3.7。

表3.7安全管理机构测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 岗位设置 | 通过访谈安全主管，检查部门/岗位职责文件，测评被测评单位的安全主管部门设置情况以及各岗位设置情况。 |
| 2 | 人员配备 | 通过访谈安全主管，检查人员名单等文档，测评被测评单位内各个岗位人员配备情况以及关键岗位的轮岗情况。 |
| 3 | 授权和审批 | 通过访谈安全主管，检查相关文档，测评被测评单位对重要活动的授权和审批情况。 |
| 4 | 沟通与合作 | 通过访谈安全主管，检查相关文档，测评被测评单位对内部部门、外部单位间的沟通与合作情况。 |
| 5 | 审核与检查 | 通过访谈安全主管，检查相关制度文档和管理要求文档等过程，测评被测评单位对安全工作的审核和检查情况。 |

**（8）人员安全管理**

人测评对象主要为安全主管人员、人事管理人员、相关管理制度、相关工作记录等，涉及工作单元5个。

各个测评指标的具体内容和测评要求见表3.8。

表3.8人员安全管理测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 人员录用 | 通过访谈人事负责人，检查人员录用文档等过程，测评被测评单位在录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。 |
| 2 | 人员离岗 | 通过访谈人事负责人，检查人员离岗要求文档等过程，测评被测评单位在人员离岗时是否按照一定的手续办理。 |
| 3 | 人员考核 | 通过访谈安全主管，检查有关考核记录等过程，测评被测评单位是否对人员进行日常的业务考核和工作审查。 |
| 4 | 安全意识教育和培训 | 通过访谈安全主管，检查培训计划和执行记录等文档，测评被被测评单位是否对人员进行安全方面的教育和培训。 |
| 5 | 外部人员访问管理 | 通过访谈安全主管，检查有关文档等过程，测评被测评单位对第三方人员(物理、逻辑)信息系统是否采取必要控制措施。 |

**（9）系统建设管理**

测评对象主要为安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等，涉及工作单元9个。

各个测评指标的具体内容和测评要求见表3.9。

表3.9系统建设管理测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 系统定级 | 通过访淡安全主管，检查系统定级相关文档等过程，测评信息系统是否按照一定要求确定其等级。 |
| 2 | 安全方案设计 | 通过访谈系统建设负责人，检查系统安全建设计划等文档．测评被测评单位对系统整体的安全规划设计是否按照一定流程进行。 |
| 3 | 产品采购 | 通过访谈安全主管、系统建设负责人，检查相关采购制度等过程，测评被测评单位是否按照一定的要求进行信息系统的产品采购。 |
| 4 | 自行软件开发 | 通过访谈系统建设负责人，检查相关软件开发文档和管理制度文档，测评被测评单位对自行开发的软件是否采取必要的措施保证开发过程的安全性。 |
| 5 | 外包软件开发 | 通过访谈系统建设负责人，检查相关文档，测评被测评单位对外包开发的软件是否采取必要的措施保证开发过程和日后的维护工作能够正常开展 |
| 6 | 工程实施 | 通过访谈系统建设负责人，检查相关制度文档和实施文档，测评被测评单位对系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。 |
| 7 | 测试验收 | 通过访谈系统建设负责入，检查相关制度文档和测试验收文档，测评被测评单位在信息系统运行前是否对其进行测试验收工作。 |
| 8 | 系统交付 | 通过访谈系统运维负责人，检查系统交付清单和系统交付管理制度等过程，测评被测评单位是否采取必要的措施对系统交付过程进行有效控制。 |
| 9 | 系统备案 | 访谈安全主管，了解系统备案及相关资料管理情况，访谈文档管理员，了解系统备案相关资料的查阅控制情况。 |
| 10 | 等级测评 | 访谈是否安排专人负责系统等级测评管理，三级系统是否每年进行测评，对测评不符合项是否及时整改。 |
| 11 | 安全服务商选择 | 通过访谈系统运维负责人，测评被测评单位是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。 |

**（10）系统运维管理**

测评对象主要为安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规范文件、执行过程记录等，涉及工作单元12个。

各个测评指标的具体内容、测评对象和测评要求见表3.10。

表3.10系统运维管理测评实施内容表

| **序号** | **测评指标** | **测评要求** |
| --- | --- | --- |
| 1 | 环境管理 | 通过访淡物理安全负责人，检查主机房安全管制度和办公环境管理文档等过程，测评被测评单位是否采取必要的措施对主机房的出入控制和办公环境的人员行为等方面进行安全管理。 |
| 2 | 资产管理 | 通过访谈资产管理员，检查资产清单和系统、网络设备等过程，测评被测评单位是否采取必要的措施对信息系统资产进行分类标识管理。 |
| 3 | 介质管理 | 通过访谈资产管理员，检查介质管理记录、介质安全管理制度以及各类介质等过程，测评被测评单位是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。 |
| 4 | 设备管理 | 通过访谈资产管理员、系统管理员，检查设备使用管理文档和设备操作规程等过程，测评被测评单位是否采取必要的措施确保设备在使用、维护和销毁等过程安全。 |
| 5 | 监控管理和安全管理中心 | 访谈运维负责人，了解监控对象范围、采用的监控工具、监控指标等情况，检查监控记录，是否记录了监控对象、监控内容、监控异常现象处理等内容。 |
| 6 | 网络安全管理 | 通过访谈安全主管、网络管理员，检查网络安全管理制度、网络审计日志和网络漏洞扫描报告等过程，测评被测评单位是否采取必要的措施对网络的安全配置，网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。 |
| 7 | 系统安全管理 | 通过访谈安全主管、系统管理员，检查系统安全管理制度、系统审计日志和系统漏洞扫描报告等过程，测评被测评单位是否采取必要的措施对信息系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。 |
| 8 | 恶意代码防范管理 | 通过访谈系统运维负责人，检查恶意代码防范管理制度和恶意代码检测、分析记录等过程，测评被测评系统是否采取必要的措施对恶意代码进行集中管理，确保信息系统具有恶意代码防范能力。 |
| 9 | 密码管理 | 通过访淡安全员，检查密码管理制度等过程，测评被测评单位是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。 |
| 10 | 变更管理 | 通过访谈系统运维负责人，检查变更方案和变更管理制度等过程，测评被测评单位是否采取必要的措施对系统发生的变更进2行有效管理。 |
| 11 | 备份和恢复管理 | 通过访谈系统管理员、网络管理员、检查系统备份管理文档和记录等过程，测评被测评单位是否采取必要的措施对数据、设备和系统进行备份，并确保必要时能够对信息系统进行有效地恢复。 |
| 12 | 安全事件处置 | 通过访谈系统运维负责人，检查安全事件记录分析文档、安全事件报告和处置管理制度等过程，测评被测评单位是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。 |
| 13 | 应急预案管理 | 通过访谈系统运维负责人，检查应急响应预案文档，应急预案培训记录等过程，测评被测评单位是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。 |

**3.整体测评与风险分析**

针对单项测评结果的不符合项，采取逐条判定的方法，从安全控制间、层面间和区域间出发考虑，给出整体测评的具体结果，并对系统结构进行整体安全测评。

依据等级保护的相关规范和标准，采用风险分析的方法分析等级测评结果中存在的安全问题可能对被测系统安全造成的影响。

**4.测评报告编制**

完成上述测评工作和招标方实施整改后，出具符合公安机关要求的（年度）保护等级测评报告。

**5.售后服务**

售后服务内容主要包括以下几个方面：

（1）管理制度完善

根据差距分析报告，分别从人员安全管理、安全管理机构、安全管理制度、系统建设管理以及系统运维管理四个方面进行梳理，协助招标方制定适宜的管理制度体系文件。

（2）技术培训

测评结束后，提供网络安全法规、网络安全防范、网络安全管理等有关的网络安全培训不少于3次，以增强招标方技术人员网络安全意识以及网络安全防范技能。

（3）安全应急

要求中标后为招标方提供日常安全技术咨询服务，必要时提供远程或现场指导。

**第二节 商务要求**

1、供应商须在谈判响应文件中提供已入围全国等级保护测评机构推荐目录在中国信息安全等级保护网官网截图。

2、异地等级测评机构须在合同签订之前完成在安徽省信息安全等级保护主管部门备案推荐工作并取得相关备案证明。

3、服务期：自合同签字之日起2个月内完成。自合同签订之日起30日内出具符合公安机关要求的信息系统安全保护测评报告以及合理的建设整改建议书,整改建议书中需对不符合信息安全等级保护三级管理规范和技术标准的系统，出具可行整改方案,协助甲方整改并提供整改项的复测服务。

4、质保期：免费质保 1 年，在质保期内为用户免费提供不少于4次的上门服务、安全巡检、软件的维护和升级。

5、付款方式：甲方验收合格后，10个工作日内向乙方支付该合同价款。

**第二节 其他要求**

（1）本项目为交钥匙工程，一次性报价，报价时应充分考虑人员费用、培训费及项目实施中的其他价格因素，投标报价包括采购、运输、人工、安装、调试、售后服务、税费等所有费用，漏报视为自动让利。

（2）投标人中标后，服务不能满足招标文件要求的，采购人有权取消中标人资格或合同，不予退还履约保证金，并按有关规定进行处理。

（3）违约责任问题，合同执行中若发生纠纷由采购人和中标人双方协商解决，协商不成通过采购人所在地仲裁或诉讼解决。

（4）遵守采购人纪律，注意保密。

（5）知识产权：中标人保证对其出售的标的物享有合法的权利，中标人应保证其所出售的标的物没有侵犯任何第三方的知识产权和商业秘密等权利。

（6）招标人将保留对预中标单位的资质、资格证明文件、投标文件的真实性进行标后核查的权力，如发现有弄虚作假行为，一律按规定上报有关监督部门做废标处理。