**国家抗肿瘤药物临床应用监测平台风险评估和等级保护测评**

**技术需求书**

## 1. 项目背景

当前网络及信息安全已经上升到国家安全层面，各级监管机构对医疗行业监管要求日趋严格，外部网络攻击数量增长迅速，产业化犯罪趋势明显，大量医疗科技新技术的应用也使医疗单位内外部网络安全形势日趋严峻。为落实关键信息基础设施防护责任，进一步提升综合安全保障能力，拟开展信息安全综合保障项目，并为各项业务发展创造安全稳定环境。

## 2.总体目标

确保国家抗肿瘤药物临床应用监测平台安全保障能力持续保持在合理水平，开展系统风险评估、等级保护测评等工作，提升信息安全综合保障能力，完善信息安全领域的发现、评估、分析、整改、监督机制，促进每个环节发挥最大作用。

## 3.招标内容

对国家抗肿瘤药物监测平台（软硬件环境）开展系统风险评估、等级保护安全测评，在此基础上对该系统信息安全状况进行综合评述，出具年度信息安全报告。为达到本项目需达到的安全服务目的和水平，服务内容包括但不限于以下内容：

#### 3.1 系统风险评估

结合我院管理、技术要求，对国家抗肿瘤药物监测平台开展全面、系统、深度的信息安全风险评估工作，采取非现场技术测试为主、现场验证为辅的工作方式，以我院相关安全规范为基础，梳理安全合规现状达标情况，验证各层各类安全机制的有效性，并在此基础上深度挖掘可能存在的安全漏洞和风险点，综合评估信息安全风险，提出合理可行的安全整改建议，并进行整改复查和跟踪反馈，最终出具年度风险评估报告。

#### 3.2 系统等保测评

结合我院管理、技术要求，依据《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息系统安全等级保护基本要求》（GB/T 22239-2008）等国家标准，通过实施等级保护测评，识别系统与国家等级保护标准要求之间的差距，并根据系统的重要程度以及安全等级保护要求提出合理的安全改进建议，增加信息系统安全规范性和有效性，提高我院人员安全意识，增强网络抗攻击能力，提高系统与相应等级化保护具体要求的符合程度，并出具等级保护测评报告。

## 4. 项目管理要求

### 4.1风险控制要求

作为信息安全服务类项目，乙方所提交方案设计与具体实施应必须满足以下原则，并在各个项目方案中逐条落实并予以详细解释：

* 最小影响原则：安全检测、渗透工作应尽可能小的影响系统和网络的正常运行，不能对现网的运行和业务的正常提供产生显著影响（包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况应在应答书上详细描述）；
* 可控性原则：方法和过程要在双方认可的范围之内，安全服务的进度要按照进度表进度的安排，保证买方对于服务工作的可控性；
* 整体性原则：安全检测、渗透内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患；乙方遗漏的安全隐患在验收后半年内造成的买方损失，买方有权追究乙方的经济赔偿。
* 标准性原则：服务方案的设计与实施应依据国内或国际的相关标准进行；
* 规范性原则：服务提供商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；
* 保密原则：对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买方的行为，否则买方有权追究乙方的责任。买方有权要求乙方在服务结束之后销毁所有和本项目有关的数据和文档。

### 4.2安全服务整体要求

1. 依据我院提供的关注要点，乙方应在标书应答时明确对关注点逐一列出评测点，并详细描述完成此关注点的整体方案，应包含但不限于技术方案和实施方案。技术方案包括整体流程、技术方法和服务方案设计等，需要对每项技术方法及部署位置进行详细描述；实施方案包括人员组织、时间安排、工具配备、阶段性文档提交、验收标准、质量保证和风险规避措施等。
2. 乙方应详细描述项目过程中人员的组成及各自职责的划分。乙方应配置有医疗行业内安全项目管理经验的管理人员进行本项目的管理工作且在乙方单位内具备中层以上职务；技术人员要求具备安全检测、渗透服务项目的丰富实施经验，我院对乙方提供的项目管理人员需进行相关内容的考核，考核通过乙方方可安排，在协商确定项目组人员组成后未经我院确认不允许随意更换。
3. 服务需要的运行环境(如设备、场地、网络环境等)由我院提供，乙方应详细描述需要的运行环境的具体要求。
4. 服务需要的测试软件、测试手机由乙方提供。

## 5.主要交付物

根据工作内容要求，项目交付包括但不限于以下内容：

|  |  |  |
| --- | --- | --- |
| **序号** | **交付物名称** | **形式** |
| 1 | 等保测评工作方案 | 电子 |
| 2 | 系统等级保护测评报告 | 电子、纸质 |
| 3 | 系统风险评估工作方案 | 电子 |
| 4 | 信息系统风险评估报告 | 电子、纸质 |

## 6.资质和材料要求

1. 具备有效期内的中国合格评定国家认可委员会颁发的“检验机构认可证书”或国家认证认可监督管理委员会颁发的“计量认证合格证书”。
2. 具备国家网络安全等级保护工作协调小组办公室颁发的“网络安全等级保护测评机构推荐证书”。
3. 2016年至2019年需完成3个合同金额大于100万的风险评估或等级保护测评相关信息安全服务项目，并提供项目案例的合同关键页及验收证明
4. 至少有3个项目实施成员中拥有在有效期内中国信息安全测评中心颁发的注册信息安全专业人员CISP证书。
5. 其他材料（非必需）：承担非涉密信息系统风险评估的测评机构在国家发改委推荐名单内（见《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知 》发改高技[2008]2071号文）。