**国家癌症中心**

**全国抗肿瘤药物临床应用监测网等保测评和安全加固服务**

**技术需求书**

## 1.项目服务原则

**（一）安全保密原则**。投标人在提供安全服务的过程中，要严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，服务过程中凡是涉及到的任何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。

**（二）最小影响原则**。投标人开展的安全服务工作，要尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如不可抗力无法避免，应对风险进行说明。

**（三）规范性原则**。投标人开展的安全服务工作，要由专业的安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

**（四）可控性原则**。投标人在开展安全服务工作过程中采用的工具、方法和过程要在双方认可的范围之内，保证用户对于服务过程的可控性。

**（五）质量保障原则**。投标人开展的安全服务工作需特别重视项目质量管理，项目的实施需严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

## 2.具体采购内容

（一）网络安全等级保护测评

1.现状调研主要内容包括：收集整理系统配置、部署、业务运行模式、网络拓扑结构、技术架构、运行环境（周边控制、安全措施）以及信息安全策略等技术方案；开展调查和现场访谈，对系统信息（包括：主机、数据库、网络设备、系统软件、中间件、安全设备等）进行记录，将所有与信息系统有关的信息资产进行核查备案。成果输出：《信息系统基础调研表》。

2.差距分析依据GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》规定的相关条款以及相关监管要求等内容，对系统的安全物理环境、安全通信网络、安全通信边界、安全计算环境、安全管理中心、安全管理制度、安全管理组织、安全管理人员、安全建设管理、安全运维管理十个层面进行差距分析，并结合漏洞扫描和渗透测试结果，分析存在的安全隐患，编制系统等级保护差距分析报告，并给出安全整改建议，指导系统安全建设整改。成果输出：《网络安全等级保护差距分析》《问题列表及整改建议》。

3.漏洞扫描采用漏洞扫描工具，对系统进行扫描，主动发现应用系统、操作系统、数据库中隐藏的漏洞，并依据结果输出漏洞描述及修补建议；采用WEB应用弱点扫描工具、数据库弱点扫描工具进行全面扫描，经人工验证后出具安全隐患清单和安全加固建议。成果输出：《系统设备漏洞扫描报告》《漏洞修补方案》《安全加固建议》。

4.渗透测试利用测试工具进行全覆盖信息采集、漏洞发现、漏洞利用等测试，并结合实战经验模拟黑客攻击信息系统，通过非破坏性质安全检测，发现信息系统隐藏的安全弱点，明确信息系统潜在风险，提供有针对性的技术保护措施。成果输出：《信息系统渗透测试报告》。

5.设计定制全体系整改方案，并配合责任主体开展整改根据等保差距分析报告、漏洞扫描报告和渗透测试报告，编写和提交信息系统等级保护改造详细设计和实施方案，经评审通过后，全程指导和协助系统安全技术体系与安全管理体系的整改建设。成果输出：《信息安全整改建设方案》《信息安全管理体系制度手册》。

6.等级保护测评

根据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）、《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）等标准，对系统进行网络安全等级保护测评。根据等级保护2.0标准的要求，测评内容包括安全物理环境、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、云计算安全扩展要求等，具体安全测评技术要求包括：1）安全物理环境测评。主要包括物理位置选择、物理访问控制、防盗和防破坏、防雷击、防火、电力供应等方面。2）安全计算环境测评。主要包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性等方面。3）安全区域边界测评。主要包括边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面。4）安全通信网络测评。主要包括网络架构、通信传输、可信验证等方面。5）安全管理中心测评。主要包括系统管理、审计管理、安全管理、集中管控等方面。6）安全管理制度测评。主要包括安全策略、管理制度、制定与发布、评审与修订等方面。7）安全管理机构测评。主要包括岗位设置、人员配备、授权和审批等方面。8）安全管理人员测评。主要包括人员录用、人员离岗、安全意识教育和培训等方面。9）安全建设管理测评。主要包括定级和备案、安全方案设计、产品采购使用、自行软件开发、外包软件开发、测试验收、等级测评等方面。10）安全运维管理测评。主要包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码管理、密码管理、备份与恢复管理、应急预案管理等方面。

成果输出：《网络安全等级保护测评报告》

（二）协助网络安全整改服务

1. 协助信息安全技术整改

投标人需协助采购人完成全国抗肿瘤药物监测网的《信息安全技术网络安全等级保护基本要求》“第三级安全等级”等保测评所有安全涉及高危漏洞整改。

2.协助信息安全管理制度整改

按照网络安全等级保护的相关要求，协助采购人建立信息安全保护持续改进机制，梳理我院现有网络安全等级保护管理制度，健全和完善我院网络安全的管理体系、技术体系和运维体系，促进信息安全保障水平不断提升。

3.协助测评

投标人在完成上述工作后，需协助采购人完成全国抗肿瘤药物监测网相关的网络安全等级保护测评工作，同时，测评报告由具备《网络安全服务认证证书等级保护测评服务认证证书》的测评机构出具。

4.安全迎检技术支持

服务有效期内根据采购人需求，配合应对上级单位所有网络安全检查，包括如下几个主要部分：

安全策略检查：检查所有安全系统安全策略，确认策略配置是否合理且有效，对不合理的配置提出整改意见，在巡检报告中给出策略优化建议。

安全漏洞排查：结合现有网络拓扑图，给出安全风险点，并给出安全加固建议。沟通业务运维流程，分析运维过程中存在的安全漏洞，提出整改建议。

依据国家信息安全等级保护相关标准，完成信息安全技术体系框架设计工作等技术支持服务；

协助采购人准备所有与全国抗肿瘤药物监测网等保相关所需材料，完善网安部门安全检查及日常工作要求的相关文件及信息录入。

**（三）商用密码应用安全性评估服务**

依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、GB/T 43206-2023《信息安全技术 信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》、《商用密码应用安全性评估量化规则（2023版）》和系统自身的安全需求，对全国抗肿瘤药物监测网进行商用密码应用安全性评估咨询工作。

具体评估技术要求包括：

1.由专业的技术人员在测评现场实地调研，在分析密码算法、技术合规性，以及密钥管理安全性的基础上，了解系统的物理环境、网络与通信环境、设备和计算情况、涉及的业务和数据等内容，了解系统的基本情况和相关密码应用等保备案情况，确定系统应采用的密码技术的相关具体环节，根据被测系统密码应用安全要求等级，选择《信息安全技术 信息系统密码应用基本要求》中的安全要求作为本次差距分析工作的基本指标，包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置共8大类别41项测评指标。由具备资质的技术人员，开展差距分析工作。

2.成果输出：《全国抗肿瘤药物监测网商用密码应用安全差距分析报告》。

## 3.资质要求

1. 具备有效的公安部第三研究所颁发的网络安全服务认证证书等级保护测评服务认证证书。
2. 具有有效的商用密码检测机构资质证书。
3. 项目组成员至少由6人（含项目经理）组成，具有专业测评证书，项目经理在本单位工作经验应不少于5年，且具有高级测评师证书,参与项目实施人员需要具备信息安全等级测评师资质。

## 4.服务承诺

1. 在项目实施过程中，应充分尊重甲方需求，采取最小影响原则和规范性原则开展工作。
2. 合同期内对发现的各类问题免费进行整改和技术支持。
3. 测评对象选择和具体实施时间以甲方要求为准。

## 5.安全保密要求

供应商要严格遵守国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，服从甲方的管理，严格遵守甲方的保密规定和工作制度，并承担相应的保密责任。

供应商所有参与本项目的服务人员须签订《保密承诺书》。供应商负责对《保密承诺书》归档保管，接受甲方检查。供应商要对承诺履行情况负有监督责任，一经发现违反承诺情况，要及时向甲方报告。

供应商所有参与本项目的服务人员自觉接受甲方的安全保密监督和管理，如违反安全保密条款，甲方将追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对泄露系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还应依法承担相应的民事责任。