**首都医科大学附属北京胸科医院2024年**

**信息化系统信息安全等级保护服务**

**采购需求**

# **项目背景**

网络安全等级保护是国家信息安全保障的基本制度、基本策略、基本方法。开展网络安全等级保护工作是保护信息化发展、维护信息安全的根本保障，是信息安全保障工作中国家意志的体现。根据《网络安全法》规定，运营、使用单位或者其主管部门应当按照网络安全等级保护制度的要求，履行网络安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改，并依据《网络安全等级保护基本要求》等技术标准，对信息系统安全等级状况开展等级测评工作。对不履行网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，对单位及直接负责的主管人员处以罚款。

# **采购目标**

我院为进一步推动网络安全等级保护工作的进展，落实《中华人民共和国网络安全法》等相关法律、法规和标准要求，计划对：1）首都医科大学附属北京胸科医院门户网站系统、2）医学影像信息系统、3）LIS系统实施网络安全等级测评，以发现其安全保护状况与相应网络安全等级保护要求之间的差距和可能存在的安全隐患，为后续系统安全建设整改和监管机构的监督管理提供参考。

# **项目总体目标**

我院将委托具有**由公安部第三研究所认证的网络安全等级测评与检测评估机构服务认证证书的**测评机构，根据等级保护基本要求，从安全技术层面和安全管理层面对下方表格内系统进行等级测评，以发现其安全保护状况与相应网络安全等级保护要求之间的差距和可能存在的安全隐患，为我院后续的系统安全建设整改和监管机构的监督管理提供参考。

|  |  |  |
| --- | --- | --- |
| **序号** | **系统名称** | **级别** |
|  | 首都医科大学附属北京胸科医院门户网站系统 | 第二级 |
|  | 医学影像信息系统 | 第二级 |
|  | LIS系统 | 第二级 |

# **项目依据**

* 《中华人民共和国网络安全法》；
* 《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)；
* 《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号文)；
* 《信息安全等级保护管理办法》(公通字[2007]43 号文)；
* 《网络安全保护等级定级指南》（GB/T22240—2020）；
* 《信息安全技术-网络安全等级保护基本要求》（GB/T22239-2019）；
* 《信息安全技术-网络安全等级保护测评要求》（GB/T 28448-2019）。

以上规范如有更新，以国家、地方、行业最新标准为准。在实施本项目期间除应遵循上述规范外，还应遵循未列出的其它法律、法规及相关国家、地方、行业标准规范。

# **项目需求**

完成北首都医科大学附属北京胸科医院2024年信息化系统信息安全等级保护服务实施范围内的所有工作，服务清单如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务名称 | 服务内容 | 工作成果 |
|  | 系统调研 | 对信息系统基本情况进行调研，包括系统责任单位信息、网络部署情况、网络设备、安全设备、服务器、数据等设备信息、配置信息，安全管理制度文档。 | 《信息系统调研表》 |
|  | 信息系统差距分析 | 依据《信息安全技术信息系统安全等级保护测评要求》和《信息安全技术信息系统安全等级保护测评过程指南》等网络安全等级保护2.0文件要求，按照等级保护基本要求所规定的检查项，对项目涉及的信息系统，逐项进行合规性检测。采用基线安全分析的方法，明确目前信息系统与等级保护要求的不符合项及差距。 | 《系统差距分析》 |
|  | 安全漏洞扫描 | 使用专业的漏洞扫描工具对信息系统进行全面漏洞扫描工作，为安全加固提供安全建议。 | 《漏洞扫描报告》 |
|  | 安全渗透测试 | 通过模拟黑客攻击的方式对用户指定的IP地址采用工具和人工检查相结合的办法进行远程安全测试，发现目标系统的安全漏洞，提供详细的渗透测试结果，并分析总结安全隐患。 | 《渗透测试报告》 |
|  | 安全整改咨询 | 根据整改建议清单中涉及安全管理部分缺失的网络安全管理制度、作业指导书和应急方案提供指导服务，指导建立更完善的网络安全基线管理制度体系。主要分为两大方面：安全技术咨询和管理制度梳理。技术咨询包含网络安全、主机安全、应用安全、数据安全。管理制度梳理包含信息安全管理机构设置、安全管理制度、人员安全管理、系统建设管理和系统运维管理五个方面。在提供安全整改建议的基础上，指导完成安全整改工作。 | 《等级保护整改建议》 |
|  | 等级保护测评 | 依据《GB/T22239-2019 信息安全技术网络安全等级保护基本要求》，围绕安全物理环境、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、安全建设管理和安全运维管理方面开展网络安全等级保护测评工作。 | 《信息系统安全等级测评报告》 |

# **测评机构资质要求**

本项目服务商需具备以下资格证书并在有效期内：

具有由公安部第三研究所认证的网络安全等级测评与检测评估机构服务认证证书；

具有中国合格评定国家认可委员会CNAS检验机构认可证书（认可的检验能力范围包含网络安全等级测评）；

具有信息安全风险评估服务资质二级及以上认证证书；

# **项目团队成员要求**

（1）服务商应为本项目成立不少于10人的项目团队，其中项目负责人1名，项目负责人应具备有效的网络安全等级测评师（高级）证书，同时具备以下证书者优先：网络空间安全类高级工程师、PMP证书、CISSP证书、注册信息安全专业人员（CISP-PTE资质证书）、CISAW证书（风险管理方向）证书。

（2）团队其他成员均应具备有效的网络安全等级测评师证书，具备以下条件者优先：至少有3名具备注册信息安全专业人员（CISP资质证书）、至少有2名具备注册渗透测试工程师（CISP-PTE证书）、至少有2名具备数据安全职业能力证书、至少有2名具备科代认证源代码检测分析工程师证书、至少有1名具备计算机技术与软件专业技术资格-信息安全工程师证书。

# **项目管理要求**

服务商在项目执行期内，应制定详细的测评工作计划，对项目执行过程提供安全、质量及进度全方位规范化服务。

服务商应严格建立质量保证体系，制定项目的质量控制方案和实施措施，并督促完成各环节质量控制内容和目标；保证项目各个阶段满足院方对质量的要求。