第八部分　服务要求及说明

一、项目概况

为落实《中华人民共和国网络安全法》的有关法律要求，提高信息系统的安全保护水平，选择具备资质的第三方专业机构，按照公安部等相关部门网络安全等级保护工作要求，对尘肺病康复站信息系统、职业健康监护(体检)系统的开展网络安全三级等级保护测评工作，同时，对采购人在用的系统开展应用安全测评工作。

通过本次工作，开展系统梳理、备案更新及等级保护测评工作，发现系统中存在的安全风险，分析系统安全现状与相关政策文件、技术标准内容要求的差距，提出安全建设整改建议，并协助采购人验证整改工作是否到位。

二、项目目标

依据《信息安全技术网络安全等级保护定级指南》(GB/T22240-2020)、《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)、《信息安全技术 网络安全等级保护测评要求》(GB/T28448-2019)、《信息安全技术 网络安全等级保护测评过程指南》(GB/T 28449-2018)等级保护相关标准，对以电子病历为核心的医院信息系统、职业健康监护(体检)系统开展定级备案、等级测评,发现系统存在的安全隐患和风险，提出可行性整改加固建议，保重要信息系统的安全防护水平满足当前和未来建设发展的安全要求,并出具《网络安全等级测评报告》。

三、服务内容

3.1 标准依据

公安部、国家保密局、国际密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)

公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》(公通字 [2007]43号)。

《信息安全技术 网络安全等级保护定级指南》(GB/T 22240-2020)

《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过程指南》(GB/T 28449-2018)

《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 可信计算规范》(GB/T 37935-2019)

《信息安全技术 大数据安全管理指南》(GB/T 37973-2019)

《信息安全技术 数据安全能力成熟度模型》(GB/T 37988-2019)

《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）

3.2 测评内容

本次等级测评项目严格按照《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）规定的测评过程实施，包括准备阶段、方案阶段、测评阶段和报告阶段。

3.2.1 等保测评内容

本次等级测评对象为尘肺病康复站信息系统、职业健康监护(体检)系统。测评工作包括但不限于以下内容：

安全技术测评：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、安全管理中心等五个方面的安全测评。

安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

安全物理环境：对系统所在物理机房安全保障情况进行测评，并根据信息系统机房和现场安全测评记录，针对机房和现场在“物理位置选择”、“物理访问控制”、“防盗窃和防破坏”、“防雷击”、“防火”、“防水和防潮”、“防静电”、“温湿度控制”、“电力供应”和“电磁防护”等安全物理环境方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

安全通信网络：根据信息系统安全通信网络测评记录，针对通信网络方面在“网络架构”、“通信传输”、“可信验证”” 等方面所采取的措施进行检查，判断出与其相对应的各测评项的测评结果。

安全区域边界：安全区域边界现场测评包括 “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”等边界区域防范措施进行检查。

安全计算环境：安全计算环境现场测评包括“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”、“数据备份恢复”、“剩余信息保护”、“个人信息保护”等几个方面的测评。

安全管理中心：安全管理中心现场测评包括“系统管理”、“审计管理”、“安全管理”、“集中控制”等方面。

安全管理制度：根据现场安全测评记录，针对信息系统在安全管理制度方面的“安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标，判断出与其相对应的各测评项的测评结果。

安全管理机构：根据现场安全测评记录，针对信息系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标，判断出与其相对应的各测评项的测评结果。

安全管理人员：根据现场安全测评记录，针对信息系统在安全管理人员方面的“人员录用”、“人员离岗”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标，判断出与其相对应的各测评项的测评结果。

安全建设管理：根据现场安全测评记录，针对信息系统在安全建设管理方面的“定级和备案”、“安全方案设计”、“产品采购和使用”、“自行软件开发”、“外包软件开发”，“工程实施”、“测试验收”、“系统交付”、“等级测评”以及“服务投标人选择”等测评指标，判断出与其相对应的各测评项的测评结果。

安全运维管理：根据现场安全测评记录，针对信息系统在安全运维管理方面的“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”、“恶意代码防范管理”、“配置管理”、“密码管理”、“变更管理”、“备份与恢复管理”、“安全事件处置”、“应急预案管理”以及“外包运维管理”等测评指标，判断出与其相对应的各测评项的测评结果。

3.2.2 应用安全测评内容

测评工作包括但不限于以下内容：

1）安全漏洞扫描：使用专业工具对被测系统进行安全漏洞检测，验证应用程序是否存在SQL注入、代码执行、文件包含、全路径泄漏等常见的安全漏洞；

2）安全功能验证：验证被测系统的身份鉴别机制是否有效、权限管理是否严密、审计功能是否健全、数据传输与存储是否安全等。

3）渗透测试：通过模拟黑客可能使用的攻击技术和漏洞发现技术，对目标系统的安全作深入的探测，测试内容包括信息收集、配置管理测试、认证测试、会话管理测试、授权测试、业务逻辑测试、数据验证测试、WEB服务测试等。

针对测试发现的安全风险项，分析并提出安全整改建议。

3.2.3 差距分析和报告出具

供应商应具备专业的风险评估能力，逐项找出系统现状与国家相关标准要求之间的差距，并针对发现的问题进行通过风险分析，给出风险处置优先级建议，形成差距分析报告。

待整改完毕后，进行结果确认，完成网络安全等级保护测评，出具测评报告，并将测评报告报当地公安机关备案。

3.2.4 成果交付

《尘肺病康复站信息系统网络安全三级等级保护测评报告》

《职业健康监护(体检)系统的网络安全三级等级保护测评报告》

在用系统的安全测评报告等交付物

3.3 团队要求

（一）供应商需根据测评业务系统的数量自行评估并配置不少于5人（全部具有等级测评师证书）的测评实施团队；供应商为本项目成立等级保护测评项目组，由项目经理统一负责，全程监督；

（二）项目经理需为高级测评师，能够有效的与采购人沟通，能按照采购人要求独立完成与业务管理相关人员的沟通协调，能够很好地执行并完成测评服务工作，并能根据一些特殊的情况可以适当增加测评服务人员，接受采购人的统一管理。

3.4 其他要求

（一）保密要求：投标人应具备保密意识及保密管理能力，项目实施过程中所收集、产生的所有与本项目相关文档、资料，包括文字、图片、表格、数字等各种形式所属权均归属采购人，成交供应商有义务对所涉及到的内容保密，并签署保密协议。

（二）培训要求：对单位信息安全人员提供培训服务，从两个维度开展培训：一是针对全员、相关人员提供网络安全意识培训，如安全事件案例介绍、安全意识知识提升；二是针对于专业技术人员提供网络安全专业知识培训，如网络安全策略基线、网络安全设备基础知识等，指导单位信息安全人员高效、合规的开展网络安全工作。

（三）维护期要求：本次等保测评工作完成且通过验收之日起1年之内提供维护服务。维护期间，如有公安机关、网信办、卫健委等监管部门对采购人在等级保护及网络安全相关方面进行检查，则按照监管要求和采购人要求，配合采购人做好相关准备工作和协助配合工作，以确保检查工作顺利开展；在维护期内，按采购人要求对在用的系统每月提供安全测评服务（包含漏扫和渗透等）。