# 附件一、项目范围及项目内容

1. 项目范围

**本次安全服务内容系统包括江苏省疾病预防控制中心主要业务系统。主要业务系统如下：**

1. 业务集成平台系统；
2. 传染病信息平台：包含法定传染病报告系统、症状监测系统、非处方药系统及用户管理中心；
3. 精神卫生平台：包含严重精神障碍信息管理系统、严重精神障碍分析报告系统以及用户管理中心；
4. 慢性病信息平台：包含死亡登记报告系统、重点慢病监测数据报告系统、慢病监测管理系统以及用户管理中心；
5. 综合业务平台管理后台；
6. 新的计划免疫系统：包括儿童接种系统、疫苗管理系统、冷链系统以及成人预防接种系统；
7. 健康教育平台：包括健康教育工作平台、健康素养学习系统以及健康素养评估系统；
8. 江苏省职业病预防信息管理平台，职防所HIS系统，职防所病案管理系统等。
9. 项目内容

本合同服务期限自2025年01月01日起至2025年12月31日止。服务期限内服务内容如下所列。

|  |  |  |  |
| --- | --- | --- | --- |
| **项目内容** | **项目说明** | **服务级别** | **输出文档** |
| 新系统上线测试 | 信息收集 | 收集网站的基本信息，如IP、域名、部署主机的操作系统、网站的开发环境等 | 10次/年 | 《XX信息系统渗透测试总结报告》 |
| 端口扫描 | 发现主机开放的敏感端口情况 |
| 弱口令测试 | 发现ssh、telnet、远程桌面、后台管理等的弱口令情况 |
| 主机漏洞测试 | 对主机进行漏洞扫描，发现主机漏洞 |
| Web漏洞测试 | 对Web应用进行非恶意性攻击测试，发现网站存在的安全问题 |
| 整改意见 | 针对发现的问题提出整改建议 |
| 安全加固服务 | 网络架构安全加固 | 梳理正确拓扑，分析不合理或不安全的因素，进行整改 | 重大活动期间及新系统上线前，不低于6次/年 | 《安全加固记录》（部分项目需要开发、管理人员配合） |
| 硬件设备安全配置加固 | 包括安全设备、网络设备、服务器安全配置的加固 |
| 操作系统安全配置加固 | 包括windows、Linux等操作系统自身安全配置的加固 |
| 软件应用安全配置加固 | 包括如MySQL、MySQL、oracle等数据库和如WebLogic、tomcat等Web中间件的安全配置加固 |
| Web应用安全加固 | 根据漏扫及渗透测试的整改意见，对网站应用进行安全加固 |
| 安全专家服务 | 对省疾控目前风险探知系统威胁分析报告 | 每季度通过省疾控风险探知系统对省疾控网络威胁进行分析并出具安全报告 | 4次/年 | 《风险探知分析报告》 |
| 应急响应服务 | 应急响应（按需） | 发生安全事件后，尽快恢复业务；如需安服介入，可找寻攻击入口点，并进行封堵 | 重大活动期间 | 《应急响应安全事故分析报告》 |

1. 项目最终交付结果

项目最终交付所呈现的结果：

|  |  |  |  |
| --- | --- | --- | --- |
| 交付结果名称 | 格式 | 急迫程度（1-5） | 特殊要求 |
| 《XX信息系统渗透测试总结报告》 | Doc | 4 |  |
| 《安全加固记录》 | Doc | 3 |  |
| 《风险探知分析报告》 | Doc | 3 |  |
| 《应急响应安全事故分析报告》 | Doc | 5 | 如有应急事故发生，产生该报告 |