**附件2**

**中心机房等保测评项目**

**技术和服务要求**

**一、项目概况**

按照《中华人民共和国网络安全法》、网络安全等级保护等相关要求进一步落实福建省无线电管理信息网网络安全防护责任，全面加强网络安全能力，提升省级无线电管理信息网的网络安全建设。

本项目目标是提升网络安全防护能力，使福建省无线电管理一体化平台（以下简称“一体化平台“）满足等级保护安全三级的安全要求，并得到相关检测部门出具的等保安全合格《测评报告》。

**二、技术和服务要求**

**（一）总体要求**

通过自身预测评与申报相关机构的等级保护测评，查找一体化平台与《信息安全技术网络安全等级保护基本要求》的差距，补缺补漏，最终获得相关测评机构出具的等保安全合格《测评报告》。

**（二）项目内容**

2.1系统等级保护定级和备案

向相关部门（网安大队）申请定级备案，按照《管理办法》和《定级指南》，初步确定定级对象的安全保护等级。初步确定信息系统安全保护等级后，聘请专家进行评审。

在定级评审通过后，向属地公安机关提交备案资料。

1、先线上提交资料审核通过后，备案单位准备好所有公安要求的纸质材料盖章，待公安通知日期携带纸质资料线下去相关公安部门网安大队进行材料递交。

2、 公安机关现场对备案材料进行审核，材料符合要求的会在两周左右颁发公安部门统一监制的备案证明。

2.2等级保护测评与加固服务

2.2.1等级保护测评服务内容

①安全技术方面

物理安全：对物理位置的选择、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、电磁防护等方面。

网络安全：对网络安全的结构安全、访问控制、安全审计、边界完整性检查、入侵防范、网络设备防护等方面进行现场测试。

主机安全：对所采用的操作系统和数据库的信息系统进行身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、资源控制等方面的测试。

应用安全：对应用系统的身份鉴别、访问控制、安全审计、通信完整性、通信保密性、软件容错、资源控制等方面进行安全测试。

数据安全及备份恢复：对信息系统的数据完整性、数据保密性和备份和恢复等方面进行测试。

②安全管理方面

安全管理制度：对信息系统的管理制度、制定和发布、评审和修订等方面。

安全管理机构：对岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等方面。

人员安全管理：对信息系统的人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等方面。

系统建设管理：对系统定级、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、安全服务商选择、系统备案、等级测评等方面。

系统运维管理：对环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等方面。

2.2.2等级保护加固服务内容

（1）资产分析服务

①根据服务范围的应用组成，派遣专业工程师到现场整理信息系统的网络结构拓扑以及相关联的资产，编制信息系统资产清单及资产报告；

②对服务范围内信息系统开展物理环境、网络结构、设备配置、应用系统以及管理制度进行调研和梳理，编制信息系统详细描述文档。

（2）风险分析服务

①对采购人信息系统常见威胁进行评估并根据等级保护要求结合单位具体情况编写单位信息安全基线库。

②通过现场评估、脆弱性评估以及渗透测试等技术手段分析信息系统安全风险以及基线差距。

③对于需要增加投资，部署新的信息安全产品和技术的整改措施，双方根据整改方案另行协商和实施。

（3）差距分析服务

在安全评估和信息系统定级的基础上，根据《信息系统安全保护等级基本要求》将定级网络环境等级保护的各项基本要求与信息安全现状进行比较分析，从管理和技术两个层面找出存在的问题并进行分析。

（4）需求分析与设计服务

①对服务范围内网络环境现状进行调研和分析，需提供至少包含现有网络环境拓扑图、网络环境架构描述及信息安全等级保护差距的基本信息。

②对服务范围内网络环境按照差距分析报告对应策略设计整改措施，面向保护对象设计安全计算环境、安全区域边界、安全通信网络等方面的整改设计方案；

③开展详细设计工作，完成网络结构框架设计、功能设计、性能设计、部署方案设计、安全策略设计等方面，形成安全整改实施规范书；

④提供信息安全等级保护建设详细方案书，应包括具体的实施内容、实施流程、风险管理和进度控制等。

（5）安全整改加固服务

①派遣专业工程师到为网站服务器实施服务器病毒检查与清理、主机安全加固、数据库安全加固建议以及进行应用安全加固；

②安全加固实施前，应提交安全加固风险分析及风险规避说明书。

（6）策略复查服务

①派遣专业工程师到现场针对加固前后的系统脆弱性进行复查，复查手段包括但不限于协议分析、漏洞扫描、漏洞验证以及配置核查等方法；

②复查结束后，形成加固前后对比复查报告。

（7）管理制度辅助建设服务

辅助采购人编写制度、各类记录表格模板等在内的三层结构的安全管理制度，达到等级保护测评要求。

2.2.3等级保护测评目标

协助采购人提交《信息系统安全等级保护测评申请书》，委托具有测评资质的机构对一体化平台进行安全等级测评，并出具正式的《信息系统安全等级保护测评报告》，一体化平台需通过网络安全等级保护测评。

2.3系统渗透和加固服务

安排安全攻防专家人员针对目标系统开展黑客模拟攻击渗透测试服务，全面检测被测系统安全性。

针对应用系统进行专家级人工的渗透测试服务，全面检测Web应用程序的安全性，深度挖掘程序中存在的各种漏洞和所面临的威胁，漏洞测试覆盖OWASP十大漏洞，如命令执行漏洞、SQL注入漏洞、XSS跨站脚本攻击漏洞、XXE漏洞、恶意代码上传漏洞、Cookie注入漏洞及其它各种敏感信息的检查等。

根据系统渗透结果对系统进行修复和加固服务。