2022年信息系统安全等级保护（三级）测评技术与服务要求

1. 投标人须使用相应等级的差距分析表格，协助采购人对整体进行分析与梳理。

2. 投标人须通过专业工具对评估范围内的系统、设备和网络进行检查。

3.根据差距分析，辅助采购人对存在的不足进行整改。

4. 投标人须根据等级保护要求，根据差距分析内容辅助采购人构建安全管理体系。

5. 投标人须配合辅助业主单位完成该信息系统等级保护安全测评，即获取测评机构出具的正式等级保护测评报告，测评结论为“中”或以上（投标人须对以上内容进行承诺，并加盖投标人公章）。

6. 投标人须依据国家《信息安全等级保护管理办法》（公通字[2007]43号）、《信息安全技术 网络安全等级保护基本要求GBT22239-2019 》、《信息安全技术 网络安全等级保护测评要求GBT28448-2019》等法规要求进行信息系统安全等级测评。

7. 物理安全测评须通过访谈、文档审查和实地察看的方式测评信息系统的物理安全保障情况。主要涉及对象为机房。

8. 安全通信网络测评须通过访谈、配置检查和工具测试的方式测评信息系统的安全通信网络保障情况。

9. 安全区域边界测评须通过访谈、配置检查和工具测试的方式测评信息系统的安全区域边界保障情况。

10. 安全计算环境须通过访谈、配置检查和工具测试的方式测评信息系统的安全计算环境保障情况。

11. 安全管理中心测评须通过访谈、配置检查的方式测评信息系统的安全管理中心保障情况。

12. 管理要求部分测评须涉及安全管理制度、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等五个方面，管理要求方面的测评对象主要为安全主管人员、安全管理人员等。

13. 安全管理制度：须针对管理制度、制定和发布、评审和修订等情况进行核查。

14. 安全管理机构：须针对岗位设置、人员配备、授权和审批、沟通和协作、审核和检查等情况进行审核。

15. 安全人员管理：须针对人员录用、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进行核查。

16. 安全建设管理：须针对系统建设的全过程，系统定级、安全方案设计等进行核查。

17. 安全运维管理：须针对资产管理、介质管理、设备管理、监控管理、系统安全管理、恶意代码防范管理、备份与恢复管理、安全事件处置、应急预案管理等进行核查。

投标人须具有公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书，如服务商属地非福建省，需要在标书中提供该分支机构在福建本地注册的营业执照复印件，并在标书中提供相关证明。测评机构所出具的测评报告须达到福建省公安厅及厦门市公安局的相关要求。

本项目测评团队需具备但不局限于以下资格：

1）、测评团队须至少具备1个高级测评师，1个中级测评师，2个初级测评师，并且由高级测评师担任项目经理。提供测评师证书复印件并加盖公章。

2）、为保证测评服务质量，需由不低于中级测评师资质的人员来担任测评过程质量监督员一职。提供承诺书并加盖公章。