附件1

**海口市人民代表大会常务委员会办公室**

**2023年网络安全等级保护测评服务要求**

**一、项目概述**

通过委托专业信息安全等级测评服务机构，根据《信息系统安全等级保护实施指南》等相关文件及标准要求，对我单位信息系统实施信息安全等级保护测评，并出具《信息系统安全等级保护测评报告》及整改指导等服务，明细如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **信息系统/服务项目** | **级别** | **重要程度** |
| 1 | 海口市人大综合管理平台 测评 | 三级 | 非常重要 |
| 2 | 海口市人大智慧会议系统 测评 | 二级 | 重要 |
| 3 | 海口市人大门户网站 测评 | 二级 | 重要 |
| 4 | 整改指导 | 测评结束后，按照国家有关规定和标准规范要求，坚持管理和技术并重的原则，向用户进行报告解读，并将技术措施和管理措施有机结合，建立信息系统综合防护体系，提供整改方案，指导用户进行整改，以达到提高信息系统整体安全保护能力。 |
| 5 | 安全漏洞扫描评估服务 | 利用扫描工具对客户的服务器主机系统与数据库系统的漏洞情况进行检查，扫描内容包括端口扫描、系统扫描、漏洞扫描、应用软件扫描等。发掘计算机信息系统网络IP网的安全漏洞，提出漏洞修补建议。 |
| 6 | 测评实施过程及结果输出 | **实施过程**：实施过程：依据《网络安全技术信息系统安全等级保护基本要求GB/T22239-2019》和《网络安全技术信息系统安全等级保护测评要求GB/T28448-2019》等相关文件及标准要求，从安全物理环境、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、安全运维管理等十个方面，按照网络安全保护等级的基本要求进行测评。**结果输出**：《信息系统安全等级保护测评报告》及提出具有针对性的整改方案。 |

**二、服务要求**

**（一）服务目标**

通过信息安全等级保护测评服务，对海口市人民代表大会常务委员会办公室的信息系统开展符合性测评，衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。找出问题，针对性的制定整改措施，推进信息安全防护体系不断完善。

**（二）信息系统安全等级保护符合性测评**

按照公安部制订的信息系统安全等级测评报告格式编制等级测评报告，报告中必须明确相应信息系统是否满足等级保护要求。

**（三）整改方案编制**

测评机构需根据测评结果，应针对性的提出整改建议方案。整改建议方案应具有可操作性，符合我单位实际情况，且能够切实解决问题。

整改建议方案应明确设计依据、整改内容、整改方案、能够解决的问题、投资概算以及风险评估。

在整改实施过程中，测评机构应全力支持，负责技术把关、整改验收以及其他咨询工作。

**（四）交付成果和报告**

中标方需在60天内交付成果和报告，提交测评报告及安全整改方案，包括：

《海口市人大综合管理平台等级测评报告》

《海口市人大综合管理平台整改建议方案》

《海口市人大智慧会议系统等级测评报告》

《海口市人大智慧会议系统整改建议方案》

《海口市人大门户网站等级测评报告》

《海口市人大门户网站整改建议方案》

测评过程材料，包括调研表、技术测评记录、会议纪要等。

**（五）服务验收标准**

服务通过验收须满足以下所有条件：

1. 完成信息系统测评并出具《测评报告》；
2. 针对性的制定整改方案，并出具《整改建议方案》；
3. 提交调研表、技术测评记录、会议纪要等服务过程材料；
4. 符合省级以上公安部门提出的信息安全等级保护测评相关要求。