

B 包采购需求书

一、项目要求

通过委托专业网络安全等级测评服务机构，根据《中华人民共和国网络安全法》、《网络安全等级保护条例》、网络安全等级保护 2.0 标准等相关文件及标准要求，对采购人信息系统进行网络安全等级保护测评，并出具《网络安全等级保护测评报告》和《网络安全等级保护整改方案》，明细如下：

序号	信息系统/服务项目	备案级别	重要程度
1	海南省应急管理厅 OA 系统	三级	非常重要
2	海南省应急管理厅门户网站	三级	非常重要
3	海南省应急管理“一张图”系统	三级	非常重要
4	应急管理“一张图”系统	三级	非常重要
5	遥感灾情辅助决策	三级	非常重要
6	海南省应急管理综合应用平台（一期）	三级	非常重要
7	海南省应急大数据可视化系统	三级	非常重要
8	海南省应急管理值班值守系统	三级	非常重要
9	危险化学品一体化监管系统	三级	非常重要
10	应急态势综合分析与指挥调度系统（一期）	三级	非常重要
11	自然灾害综合监测预警系统	三级	非常重要
12	信息接入与会商决策系统测评	二级	非常重要
13	应急通讯融合系统测评	二级	非常重要
14	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，针对测评报告进行解读，并将技术措施和管理措施有机结合，建立网络安全综合防护体系，提供整改方案，协助指导整改，以达到提高网络整体安全保护能力。	
15	结果输出	一、《网络安全等级保护测评报告》	

二、建设目标

按要求完成应急管理信息系统网络安全等级保护测评，并提交相关系统的测评报告和整改报告。

三、服务内容

1、等保测评服务内容和流程

1.1 测评内容

委托符合国家要求的专业机构依据《信息系统安全等级保护基本要求》，落实物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施，落实安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等安全保护管理措施，具体内容如下图所示：

信息系统安全等级保护基本要求			
技术要求		管理要求	
物理安全	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	主机安全	身份鉴别 访问控制 安全审计 剩余信息保护 入侵防范 恶意代码防范 资源控制
	网络安全		结构安全 访问控制 安全审计 边界完整性检查 入侵防范 恶意代码防范 网络设备防护
		数据安全与备份恢复	数据安全
数据完整性 数据保密性 备份和恢复	应用安全		安全管理机构
			安全管理制度
			安全管理机构
			系统建设管理
			人员安全管理
			系统运维管理
			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
			管理制度制定和发布 评审和修订
			岗位设置 人员配备 授权和审批 沟通和合作 审核和检查
			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 系统备案 等级测评 安全服务商选择

图 1 测评内容图

1.2 测评流程

对信息系统等级保护测评实施的基本流程见图：

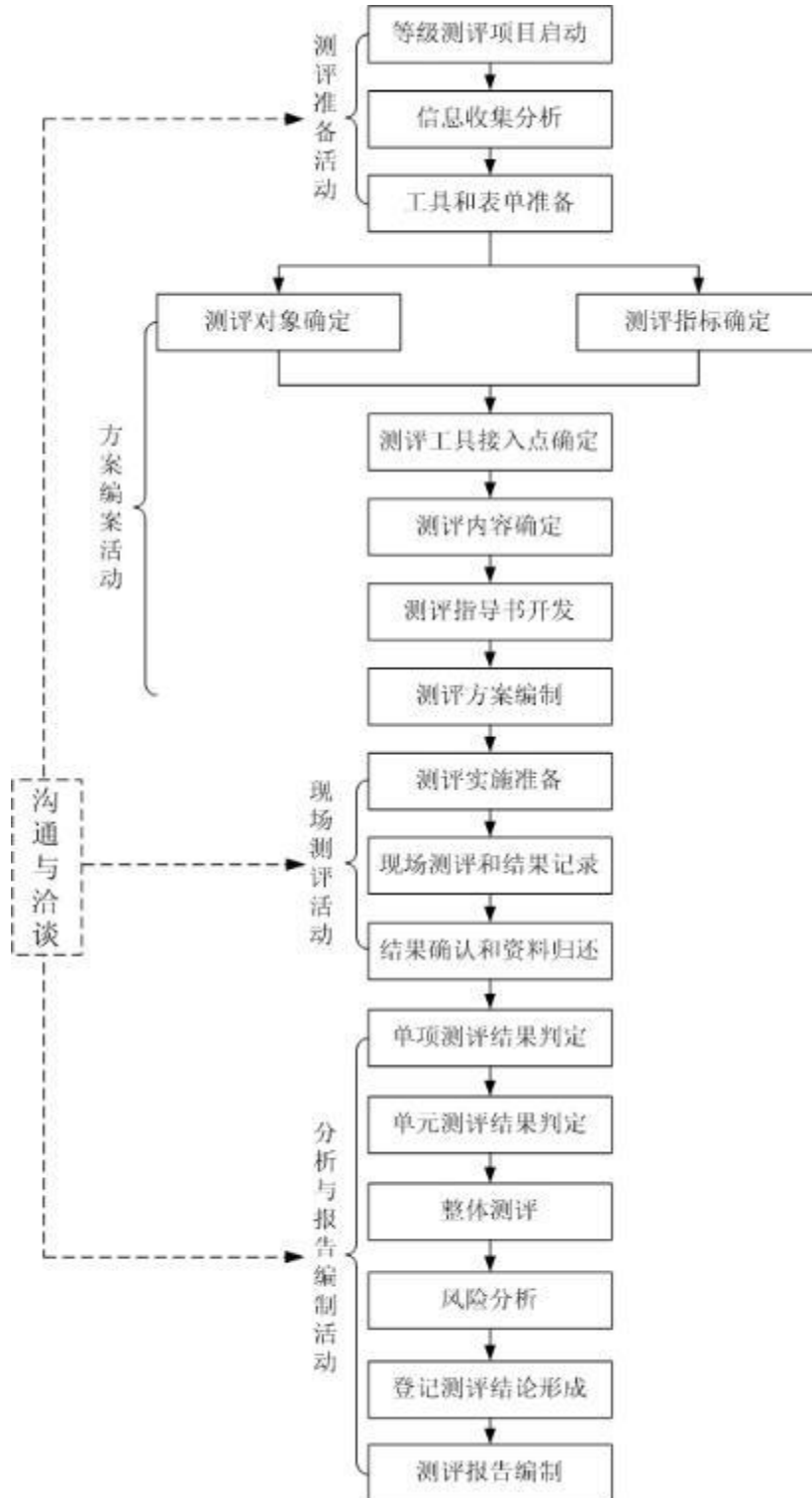


图 2 测评流程图

为确保等级测评工作的顺利开展，应首先明确等级测评的工作流程，然后按工作流程中的活动内容有序地开展等级测评工作。由于不同安全保护等级信息系统的重要程度不同，安全保护力度不同，从国家等级保护的角度出发，等级测评的关注角度也应有所差异。

等级测评过程可以分为四个活动内容：测评准备活动、方案编制活动、现场测评活动和报告编制活动，而测评双方之间的沟通与洽谈应贯穿整个等级测评过程。在方案编制活动中，测评对象确定和测评指标确定两个任务可以并行。

1.3 测评指标

本次被测三级系统信息系统的安全保护依据信息系统确定的业务网络安全保护等级和系统服务安全保护等级要求，选择《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）中对应级别的安全要求作为以上信息系统等级测评的测评指标，3级测评指标为：71个控制点、211个要求项。

测评指标（三级）			
技术/管理	层面	控制点	要求项
安全技术	安全物理环境	10	22
	安全通信网络	3	8
	安全区域边界	6	20
	安全计算环境	11	34
	安全管理中心	4	12
安全管理	安全管理制度	4	7
	安全管理机构	5	14
	安全管理人员	4	12
	安全建设管理	10	34
	安全运维管理	14	48
合计		71	211

本次被测二级系统信息系统的安全保护依据信息系统确定的业务网络安全保护等级和系统服务安全保护等级要求，选择《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）中对应级别的安全要求作为以上信息系统等级测评的测评指标，2级测评指标为：68个控制点、135个要求项。

测评指标（二级）			
技术/管理	层面	控制点	要求项
安全技术	安全物理环境	10	15
	安全通信网络	3	4
	安全区域边界	6	11
	安全计算环境	10	23
	安全管理中心	2	4
安全管理	安全管理制度	4	6
	安全管理机构	5	9
	安全管理人员	4	7
	安全建设管理	10	25
	安全运维管理	14	31
合计		68	135

2、信息安全等级保护咨询及安全整改加固方案

等保测评完成后，依据测评结果进行整改设计和安全域划分，针对主机服务器、网络设备及安全设备的安全提交加固设计方案，以指导信息系统安全加固工作，消除安全隐患和主要风险点，建设具有海南应急管理信息系统特色的信息安全等级保护深度防御体系。

四、采购标的执行标准

本项目实施过程应遵循包含但不限于以下标准：

1. ITSS 体系 IT 服务标准。
2. 《ISO/IEC 20000-1：2011 信息技术-服务管理-第 1 部分：规范》；
3. GB 17859-1999 《计算机信息系统安全等级保护划分准则》
4. GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》
5. GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》
6. GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》
7. GB/T 25058 - 2019 《信息安全技术 网络安全等级保护实施指南》
8. GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》
9. T/ISEAA 001-2020 《网络安全等级保护测评高风险判定指引》

10. GB/T 21052-2016 《信息系统物理安全技术要求》；
11. GB/T25070-2019 《信息安全技术—网络安全等级保护安全设计技术》；
12. GB/T 20271-2016 《信息系统通用安全技术要求》；
13. GB/T 20984-2016 《信息安全风险评估规范》；
14. GB/Z 20985-2017 《信息安全事件管理指南》；
15. GB/T20271-2016 《信息安全技术信息系统安全通用技术要求》；
16. 《关键信息基础设施安全保护条例》
17. 《政府信息系统政府采购管理暂行办法》
18. GB/T 18336-2015 《信息技术 安全技术 信息技术安全性评估准则》
19. GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》
20. GB/T 18336-2015 《信息技术安全技术 信息技术安全性评估准则》
21. GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》
22. GM/T 0024-2014 《SSL VPN 技术的规范》
23. GM/T 0025-2014 《SSL VPN 网关产品规范》
24. GM/T 0026-2014 《安全认证网关产品规范》

五、其他内容

1、**报价要求：**应为人民币含税包干价，包含人工费、材料费、交通费、评审费用、税费等所有相关工作所发生的一切费用，采购人将不再额外支付任何费用。

2、**合同履行期限：**测评机构需在 2024 年 10 月底前交付成果和报告。

3、**合同履行地点：**采购人指定地点

4、**采购标的的验收标准及方式：**按国家相关法律及行业规定以及招标文件要求进行验收。要求完成应急管理信息系统网络安全等级保护测评工作，并提交测评报告和整改报告。

5、**付款方式：**

5.1、合同签订后预付 50%；

5.2、完成全部工作内容提交相应成果后支付 50%；