用户需求书

一、项目概况

1、项目名称：海南省卫生健康信息系统等保测评

2、本项目预算金额：58.5 万元

3、服务期限：合同签订后 120 日内交付成果和报告。

4、服务地点：采购人指定地点

二、项目背景

依据《信息安全等级保护管理办法》（公通字[2007]43 号）、《海南省深化信息安全等级保护工作方案》（琼等保办[2010]3 号）和《海南省信息化条例》文件的要求规定和建议，需委托具备资质的信息安全等保测评机构，对海南省卫生和计划生育委员会统计信息中心的相关信息系统进行等级测评服务，以确保信息系统是否在符合相对应的信息安全等级下运行。招标人开展信息安全等级保护测评工作，通过本次招标聘请具备相关资质的单位提供测评及相关支持服务，出具和相关信息系统相对应的等保测评报告。

三、项目服务内容

招标人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，针对正在运行的信息系统实施信息安全等级保护测评，明细如下：

序号	信息系统/服务项目	级别	重要程度
1	海南省出生实名信息系统	三级	非常重要
2	海南省计划生育服务站管理系统	三级	非常重要
3	海南省免疫规划管理及疫苗流通信息系统	三级	非常重要
4	海南省区域妇幼保健管理系统	三级	非常重要
5	海南省全员人口统筹管理信息系统（“金人工程”）	三级	非常重要
6	海南省卫生计生委门户网站信息系统	三级	非常重要

7	120 指挥调度系统	三级	非常重要
8	海南省智慧医院服务平台	三级	非常重要
9	健康证管理系统	三级	非常重要
10	远程会诊系统	三级	非常重要
11	海南省居民健康卡综合管理平台	拟定三级	非常重要
12	定级备案	对本单位海南省居民健康卡综合管理平台进行调研，协助编写定级报告，办理等保备案。	
13	渗透测试	通过模拟黑客可能使用的攻击方式和漏洞挖掘行为进行渗透测试，对目标信息系统的安全进行深入安全检测、评估。渗透测试的目的是通过直观的让信息系统管理人员了解自身信息系统所面临的安全问题，看到对这些漏洞的利用或攻击可以产生什么样的破坏及影响。同时，为用户信息系统管理人员提供安全加固建议，及时采取必要的安全防范措施，帮助其更好的保护信息系统，保证信息系统安全、稳定运行。在完成渗透测试服务后，提交《信息系统渗透测试报告》。服务对象：甲方指定的 5 个三级信息系统（海南省全员人口统筹管理信息系统（“金人工程”）、海南省免疫规划管理及疫苗流通信息系统、海南省区域妇幼保健管理系统、海南省智慧医院服务平台、海南省居民健康卡综合管理平台）和网站；服务次数总计：1 次/年。	
14	测评实施过程及结果输出	**实施过程**：依据《信息系统安全等级保护基本要求》实施等级测评，对物理机房、网络结构、信息系统等进行合规性检查，发现信息系统与安全保护等级要求之间的差距（包括根据需要进行异地现场测评服务）； **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。	
15	整改建议和指导	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。	

四、服务实施

（一）服务目标

通过信息安全等级保护测评服务，对本单位运行的信息系统开展符合性测评

和安全服务，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）测评依据

《信息系统安全等级保护基本要求》

《信息系统安全等级保护测评要求》

《信息系统安全等级保护测评过程指南》

（三）实施团队要求

投标人在投标文件中应提供完整的测评实施团队名单及职责分工，所有人员必须属于投标单位在册员工（以社保缴纳证明为认定依据）。实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《信息安全等级测评师证书》。测评实施团队名单中所列人员的社保缴纳证明和《信息安全等级测评师证书》复印件须在投标文件中提供，并加盖公章。

（四）服务内容

服务期内，投标人须向招标人提供以下服务。

1、等级保护培训咨询服务

1）等级保护政策/标准咨询

随着国家信息安全等级保护的推进工作，信息安全等级保护政策、法律法规和标准体系也会相应的发布和更新，投标人应针对本项目设立信息安全等级保护咨询平台，明确较为固定的咨询服务人员，并根据咨询要求提供正式的答复资料和文档。咨询内容包括但不限于信息安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

2）信息系统等级变更咨询

在信息系统出现等级变更时，投标人须协助招标人对信息系统进行分析，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

3）等级保护建设整改咨询

按照信息系统安全总体方案要求，投标人须结合信息系统安全建设项目计划，根据信息安全等级保护相关标准和规定，对招标人等级保护建设整改工作提

供全面的安全方案的详细设计咨询，结合招标人的实际情况，协助招标人进行分布或分期地落实安全技术与管理措施，并根据预期实现的安全目标，全程提供在建安全设备和系统的测试、验收工作等咨询服务。

4）信息系统安全检查咨询

在招标人开展信息系统安全检查时，全程提供咨询服务，包括检查范围、检查方法、检查结果分析以及整改措施制定等。

5）等级保护测评咨询

测评过程中，投标人应协助用户单位参照《信息系统安全等级保护测评要求》中评估内容和方法，对测评过程中所涉及到的评估项及测评过程中所编制相关表格、填写项提供全程咨询服务，确保测评工作的顺利开展。

6）相关政策、法规、技术标准的培训。

投标人应向甲方提供完整的培训方案，对信息安全等级保护相关政策、法规、技术标准进行全面培训。

2、等级保护测评服务

依据《信息系统安全等级保护基本要求》，对招标人各信息系统的安全技术体系和安全管理体系等进行合规性检查，出具《信息系统安全等级保护测评报告》，并提出具有针对性的整改建议。

1）测评内容

（1）对招标人所需测评的信息系统进行摸底、分析和梳理，提出详细的等保测评方案。

（2）逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

①　安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据备份及恢复等五个方面的安全测评；

②　安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

（3）完成测评工作后，提出整改建议；最后出具符合公安部门要求的信息系统安全保护等级测评报告，并在后期整改实施过程中提供全程咨询服务。

2）测评实施

信息安全测评项目过程需按照《信息系统安全等级保护测评过程指南》开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

（1）测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1.组建测评项目组	向用户提交 《项目计划书》 《提供资料清单》
	2.编制《项目计划书》	
	3.确定招标人应提供的资料	
信息收集分析	定级报告及整改方案分析	《系统基本情况分析报告》
	1.整理调查表单	
	2.发放调查表单给招标人	
	3.协助招标人填写调查表	
	4.收回调查结果	
	5.分析调查结查	
工具和表单准备	1.调试测评工具	确定测评工具（测评工具清单） 《现场测评授权书》 《测评结果记录表》 《文档交接单》
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

（2）方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
二、测评指标	识别被测系统业务信息和系统服务安全保护等	《测评方案》的测

确定	级	评指标部分
	选择对应等级的 ASG 三类安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
三、工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
四、测试内容确定	识别每个测评对象对象的测评指标	《测评方案》的单项测评实施和系统测评实施部分
	识别每个测评对象对应的每个测试指标的测试方法	
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向用户提交 《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

（3）现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。详细要求见下表：

工作内容	工作详细任务	输出
1.现场测评准备	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	

	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等资料更新	
2.现场测评和结构记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果：管理安全测评的测评结果记录 配置检查结果： 技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果： 技术安全测评的物理安全和管理安全测评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
3.结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	
	测评人员归还借阅的各种资料	

（4）报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。详细要求见下表：

工作内容	工作详细任务	工作依据
1.单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	

2.单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部分
	判定每个测评对象的单元测评结果	
3.整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	等级测评报告的系统整体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告提交用户
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

3、渗透测试

渗透测试是指在获取用户授权后，通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用的安全测试方法。这种测试方法可以非常有效的发现最严重的安全漏洞，尤其是与全面的代码审计相比，其使用的时间更短，也更有效率。在测试过程中，用户可以选择渗透测试的强度，例如不允许测试人员对某些服务器或者应用进行测试或影响其正常运行。通过对某些重点服务器进行准确、全面的测试，可以发现系统最脆弱的环节，以便对危害性严重的漏洞及时修补，以免后患。

（五）服务要求

1、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。

2、整改方案编制

投标人需根据测评结果，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，符合招标人实际情况，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，投标人应全力支持，负责技术把关、整改验收以及其他咨询工作。

3、成果交付

成果交付期：中标方需在合同签订后 120 日内交付成果和报告。

交付成果内容：包括（但不限于以下内容）：

信息系统定级相关文件和报告；

信息系统测评报告及整改建议方案；

信息系统漏洞扫描报告；

信息系统渗透测试报告；

制度编制报告；

人员信息安全技能培训计划。提供安全管理、测评方法、测评结果分析及整改技能等相关培训。

提供测评过程相关文件，包括调研表、技术测评记录、会议纪要等。

4、服务验收标准

服务通过验收须满足以下所有条件：

完成信息系统测评并出具《测评报告》

针对性的制定整改方案，并出具《整改建议方案》

提交调研表、技术测评记录、会议纪要等服务过程材料

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

五、售后服务及其它要求

投标人必须提供详细的保修期内技术支持和服务方案，技术支持和服务方案包括（但不限于）：

（1）如在测评中出现不符合项，中标人需要提供相应的整改建议及相关方案。对于测评中发现的主机和网络设备漏洞，投标方应提供项目验收后一年的跟踪服务，对本次评估范围内的问题提供远程技术咨询，对于漏洞的修补、问题的排除给出建议和指导，自项目验收通过之日起计算。

（2）提供服务期内，7×24 小时技术支持和服务，8 小时内作出实质性响应，对重大问题提供现场技术咨询支持，24 小时内到达指定现场。问题解决后 24 小时内，提交问题处理报告，说明问题种类、问题原因、问题解决中使用的方法及造成的损失等情况。