第三章　　采购需求

D 包采购需求—智慧洋浦（一期）项目--智慧口岸（一期）

（HNZC2021-027-003DEF）网络安全等级保护测评

一、商务要求

1、项目工期：采购人下达测评通知书后 60 日内交付《智慧洋浦（一期）项目--智慧口岸（一期）测评服务评估报告》。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：

4.1 首付款：签订合同后 15 个工作日内支付合同款的 40%。

4.2 尾款：智慧洋浦（一期）项目--智慧口岸（一期）通过竣工验收后支付合同款的 60%，当年预算不足部分顺延次年财政预算下达后支付。

4.3 项目费用参考省财政厅实际下达项目建设经费；各阶段付款时间和金额以省财政厅年度资金下达情况为准，不足部分待次年财政预算下达后支付。

注：具体以签订合同为准。

5、申请人的资格要求：见招标公告。

6、其他要求：

6.1 智慧洋浦（一期）项目--智慧口岸（一期）项目建设包及监理包已招标完成，项目实施过程中等级保护测评单位需积极配合以上单位以便顺利完成测评工作。

6.2 投标人可同时投 D、E、F 包，但最多只能中标一个包。当投标人所投 D、E、F 包综合得分均为第 1 名时，评标委员会将优先确定其中标 D 包，E 包（或 F 包）则由综合得分第 2 名的投标人中标，以此类推。

二、服务要求

1、标包名称

智慧洋浦（一期）项目--智慧口岸（一期）网络安全等级保护测评

2、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，需委托具备资质的等保测评机构，对信息系统进行等级测评，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。招标人将依照智慧洋浦（一期）项目--智慧口岸（一期）的信息系统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。

3、项目内容

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：

<table>
<tr><th>序号</th><th colspan="2">信息系统/服务项目</th><th>级别</th><th>重要程度</th></tr>
<tr><td>1</td><td colspan="2">智慧洋浦（一期）项目--智慧口岸（一期）（智慧港口平台、智慧口岸平台、智慧监管平台、智慧物流平台、智慧风控平台）</td><td>三级</td><td>非常重要</td></tr>
<tr><td>2</td><td>测评实施过程及结果输出</td><td colspan="3">实施过程：根据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》和《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》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。</td></tr>
<tr><td>3</td><td>整改指导</td><td colspan="3">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</td></tr>
</table>

		户进行整改，以达到提高信息系统整体安全保护能力。

3、服务实施

3.1 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，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。

3.2 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》

3.3 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。

4、服务内容

服务期内，投标人须向招标人提供以下服务。

4.1 等级保护咨询服务

4.1.1 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。

4.1.2 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。

4.1.3 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。

4.1.4 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。

4.1.5 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。

4.2 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。

4.2.1 测评内容

（1）对本单位已备案信息系统进行摸底、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。

4.2.2 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	《测评方案》的测评对象部分

	确定测评对象	
二、测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	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（模版）
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	

5、服务要求

5.1 等级保护测评服务

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。

5.2 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。

5.3 交付成果和报告

成果和报告，包括（但不限于以下内容）：

5.3.1《智慧洋浦（一期）项目--智慧口岸（一期）测评服务评估报告》

5.3.2《智慧洋浦（一期）项目--智慧口岸（一期）等级保护安全整改建议方案》

5.3.3 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

5.4 服务验收标准

服务通过验收须满足以下所有条件：

5.4.1 完成信息系统测评，并出具《测评报告》；

5.4.2 针对性的制定整改方案，并出具《整改建议方案》；

5.4.3 针对性的制定安全制度，并出具《安全管理制度》；

5.4.4 提交调研表、技术测评记录、会议纪要等服务过程材料；

5.4.5 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。

6、售后服务及其它要求

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

6.1 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。

6.2 提供及时有效的售后服务，中标人在本地有服务机构或承诺如果中标则在海南省设置有不少 2 名技术人员的售后服务技术支持团队，并承诺提供的售后保障计划应包含 7*24 小时的技术支持服务，重大活动期间提供现场的技术支持服务，针对突发应急事件提供 4 小时内到现场处置的服务响应保障，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。提供承诺函。

E包采购需求—智慧洋浦（一期）项目--智慧口岸（一期）

（HNZC2021-027-003DEF）第三方软件测试

一、商务要求

1、项目工期：采购人下达测试通知书后60日内交付成果和软件测试报告。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：

4.1 首付款：签订合同后15个工作日内支付合同款的40%。

4.2 尾款：在乙方出具《软件测试报告 》并验收合格后15 个工作日内，甲方支付合同款剩余部分的60%。

4.3 项目费用参考省财政厅实际下达项目建设经费；各阶段付款时间和金额以省财政厅年度资金下达情况为准，不足部分待次年财政预算下达后支付。

注：具体以签订合同为准。

5、申请人的资格要求：见招标公告。

6、其他要求：

6.1 智慧洋浦（一期）项目--智慧口岸（一期）项目建设包及监理包已招标完成，项目实施过程中软件测试单位需积极配合以上单位以便顺利完成测试工作。

6.2 投标人可同时投D、E、F包，但最多只能中标一个包。当投标人所投D、E、F包综合得分均为第1名时，评标委员会将优先确定其中标D包，E包（或F包）则由综合得分第2名的投标人中标，以此类推。

二、服务要求

在智慧洋浦（一期）项目--智慧口岸（一期）所涉及软件系统开发完成并通过初验后，对本项目所涉及的软件系统按照项目承建单位的合同条款，以及相关的国际、国家和行业的质量标准，对相关信息系统进行功能、性能、安全性等方面进行软件验收测试，并出具《软件测试报告》。

1、技术标准

GB/T 25000.51-2016 《系统与软件工程 系统与软件质量要求和评价

（SQuaRE） 第 51 部分：就绪可用软件产品（RUSP）的质量要求和测试细则》

2、测试原则

客观性和公正性原则：虽然评估工作不能完全摆脱个人主张或判断，但评估人员应当没有偏见，在最小主观判断情形下，按照评估双方相互认可的评估方案，基于明确定义的评估方式和解释，实施评估活动。

可再现性原则：不论谁执行评估，依照同样的要求，使用同样的评估方式，对每个评估实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同评估者评估结果的一致性有关，后者与同一评估者评估结果的一致性有关。

结果完善性原则：评估所产生的结果应当证明是良好的判断和对评估项的正确理解。评估过程和结果应当服从正确的评估方法以确保其满足了评估项的要求。

3、测试对象及范围

序号	系统名称
1	智慧洋浦（一期）项目--智慧口岸（一期）

4、测评内容应当涉及以下内容：

包括软件功能性、可靠性、易用性、效率、维护性、移植性等质量特性。

4.1 功能性测试

软件产品满足明确和隐含要求功能的能力。具体内容包括：完备性、正确性、恰当性、互操作性、安全保密性等。

4.2 可靠性测试

软件产品维持规定的可靠性级别的能力。按照软件运行剖面对软件进行随机测试的测试方法。具体内容包括：成熟性、容错性、易恢复性等。

4.3 易用性测试

软件产品被理解、学习、使用和吸引用户的能力。关注软件使用时是否感觉方便，能否通过简单的操作达到用户的目的，界面是否美观，排版是否合理等。具体内容包括：易理解性、易学性、易操作性、吸引性等。

4.4 效率性能测试

软件产品所提供性能的能力。关注在多用户、大并发量的情况下系统是否满足客户的实际需要，主要从吞吐量、点击率、平均事物响应时间、负载下的平均

事物响应时间等来进行测试。具体内容包括：时间特性、资源利用率、容量等。

4.5 维护性测试

软件产品可被修改的能力。修改可能包括修正、改进或软件适应环境、需求和功能规格说明中的变化。具体内容包括：易分析性、易改变性、稳定性、易测试性、维护性依从性。

4.6 移植性测试

软件产品从一种环境迁移到另外一种环境的能力。具体内容包括：适应性、易安装性、共存性、易替换性、可移植性依从性等。

4.7 用户文档测试

用户文档是否包含使用该软件所必须要的信息、所陈述的功能以及最终用户能调用的功能、可靠性特征及其操作、可能导致数据丢失的系统终止或结束条件、是否给出必要数据的备份和恢复指南、对所有关键功能是否提供完备的细则信息和参考信息等，便于用户使用、操作、维护等。用户文档及相关材料是否有软件实际相符。

5、项目具体要求

5.1 实施要求

5.1.1 系统梳理

对本次测评多设计软件系统进行梳理，了解软件系统的主要业务应用、系统架构等情况。

5.1.2 现场测评

对本项目所涉及软件系统进行现场测试，出具缺陷报告，待开发单位整改后进行回归测试。

5.1.3 成果递交

整理测试结果，出具软件测试报告。

5.2 实施过程风险管理

测试实施过程中，被测系统可能面临业务中断、数据丢失等安全风险，投标方应就可能存在的风险进行充分识别并采取必要的规避或防范措施。

5.3 项目管理与实施保障

对项目进行科学严格的管理，通过系统计划、有序组织、科学指导和有效控制，促进项目全面顺利实施，投标人必须提供完整的项目管理方案，并符合以下

要求：

5.3.1 投标人及其测试人员应当严格执行有关国家信息安全相关标准和有关规定，提供客观、公平、公正的服务；测试过程中其相关人员应注意测试记录和证据的接收、处理、存储和销毁，保护其在测试期间免遭改变/遗失，并保守秘密；

5.3.2 配置相应的项目经理、技术主管、质量主管、技术人员等，参与此次测试服务的投标人其评估人员应具备并符合以下要求：

5.3.2.1 仅限于中华人民共和国境内的中国公民，且无犯罪记录；

5.3.2.2 取得网络安全测试评估相关资质证书；

5.3.2.3 具备从事信息系统安全评估相关工作经验。

F包采购需求—智慧洋浦（一期）项目--智慧口岸（一期）（HNZC2021-027-003DEF）密码保护测评

一、商务要求

1、项目工期：采购人采购人下达评估通知书后90日内交付《智慧洋浦（一期）项目--智慧口岸（一期）密码应用安全性评估报告》。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：

4.1 首付款：签订合同后15个工作日内支付项目密码测评费的40%。

4.2 尾款：智慧洋浦（一期）项目--智慧口岸（一期）通过竣工验收后支付项目密码测评费的60%，当年预算不足部分顺延次年财政预算下达后支付。

4.3 项目费用参考省财政厅实际下达项目建设经费；各阶段付款时间和金额以省财政厅年度资金下达情况为准，不足部分待次年财政预算下达后支付。

注：具体以签订合同为准。

5、申请人的资格要求：见招标公告。

6、其他要求：

6.1 智慧洋浦（一期）项目--智慧口岸（一期）项目建设包及监理包已招标完成，项目实施过程中密码保护测评单位需积极配合以上单位以便顺利完成密码保护测评工作。

6.2 投标人可同时投D、E、F包，但最多只能中标一个包。当投标人所投D、E、F包综合得分均为第1名时，评标委员会将优先确定其中标D包，E包（或F包）则由综合得分第2名的投标人中标，以此类推。

二、服务要求

1、标包名称

智慧洋浦（一期）项目--智慧口岸（一期）密码保护测评

2、项目目标

根据《中华人民共和国密码法》、《商用密码管理条例（修订草案征求意见稿）》、《商用密码应用安全性评估管理办法（试行）》以及国家关于重要领域密码应用

的有关要求，通过对智慧洋浦（一期）项目--智慧口岸（一期）在通用要求、商用密码应用技术要求、密码应用管理要求方面的评估，对系统商用密码应用的合规性、正确性、有效性作出判断，给出系统在商用密码技术应用、密钥管理及安全管理方面与其相应安全等级信息系统密码应用基本要求之间的差距，最终出具被评估系统的密码应用安全性评估报告。

3、项目对象

序号	系统名称	系统等级
1	**智慧洋浦（一期）项目--智慧口岸（一期）**	三级

4、服务内容

本项目包括对智慧洋浦（一期）项目--智慧口岸（一期）进行商用密码应用安全性评估服务（含密码应用方案评估、系统评估），最终输出被评估系统的密码应用方案评估报告、密码应用安全性评估报告，满足商用密码应用安全性评估工作的验收要求，具体内容包括：

序号	服务内容	服务内容子项	工作内容
1	需求沟通确认	需求沟通调研和确认工作实施要求	对安全评估的组织实施流程、风险管控效果、时间节点、交付成果、评估方式等基础信息进行沟通核实，确认服务需求和工作要求
2	基础材料搜集整理和现场沟通采集	按照评估准备实施要求，搜集整理必要素材	通过远程或现场会议方式与业务研发、运维部门技术团队和保障团队沟通评估所需基础素材、文档等必要信息
3	密码应用方案评估	密码应用方案评估	对委托方制定的密码应用方案进行评估，出具《密码应用方案评估报告》

4	系统评估	依据 GB/T 39786-2021《信息系统密码应用基本要求》等标准进行测评	按照 GB/T 39786-2021《信息系统密码应用基本要求》及通过评估的密码应用方案对系统进行评估，采取材料审查、人员访谈、实地查看、配置检查、工具测评等评估方法对系统密码应用情况进行评估分析，核查系统技术应用、密钥管理、安全管理是否符合密评要求。
5	报告编制	编制评估报告	对评估过程中发现的问题进行汇总确认，总结各项评估指标的评估结果，编制评估报告。

5、评估内容

针对智慧洋浦（一期）项目--智慧口岸（一期），开展商用密码应用安全性评估，从通用要求、物理和环境、网络和通信、设备和计算、应用和数据、管理制度、人员管理、建设运行、应急处置等方面开展测评，具体测评指标如下（以等级保护第三级信息系统为例）：

测评层面	测评单元	指标要求
物理和环境安全	身份鉴别	1.1 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。
	电子门禁记录数据存储完整性	1.2 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性。
	视频监控记录数据存储完整性	1.3 宜采用密码技术保证视频监控音像记录数据的存储完整性。
网络和通信安全	身份鉴别	2.1 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。
	通信数据完整性	2.2 宜采用密码技术保证通信过程中

		数据的完整性。
	通信过程中重要数据的机密性	2.3 应采用密码技术保证通信过程中重要数据的机密性。
	网络边界访问控制信息的完整性	2.4 宜采用密码技术保证网络边界访问控制信息的完整性。
	安全接入认证	2.5 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。
设备和计算安全	身份鉴别	3.1 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。
	远程管理通道安全	3.2 远程管理设备时，应采用密码技术建立安全的信息传输通道。
	系统资源访问控制信息完整性	3.3 宜采用密码技术保证系统资源访问控制信息的完整性。
	重要信息资源安全标记完整性	3.4 宜采用密码技术保证设备中的重要信息资源安全标记的完整性。
	日志记录完整性	3.5 宜采用密码技术保证日志记录的完整性。
	重要可执行程序完整性、重要可执行程序来源真实性	3.6 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。
应用和数据安全	身份鉴别	4.1 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。
	访问控制信息完整性	4.2 宜采用密码技术保证信息系统应用的访问控制信息的完整性。
	重要信息资源安全标记完整性	4.3 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；

	重要数据传输机密性	4.4 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。
	重要数据存储机密性	4.5 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。
	重要数据传输完整性	4.6 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。
	重要数据存储完整性	4.7 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
	不可否认性	4.8 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。
管理制度	具备密码应用安全管理制度	5.1 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
	密钥管理规则	5.2 应根据密码应用方案建立相应密钥管理规则；
	建立操作规程	5.3 应对管理人员或操作人员执行的日常管理操作建立操作规程；
	定期修订安全管理制度	5.4 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
	明确管理制度发布流程	5.5 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
	制度执行过程记录留存	5.6 应具有密码应用操作规程的相关

		执行记录并妥善保存。
人员管理	了解并遵守密码相关法律法规和密码管理制度	6.1 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
	建立密码应用岗位责任制度	6.2 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限： 1）根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2）对关键岗位建立多人共管机制； 3）密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任； 4）相关设备与系统的管理和使用账号不得多人共用。
	建立上岗人员培训制度	6.3 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
	定期进行安全岗位人员考核	6.4 应定期对密码应用安全岗位人员进行考核；
	建立关键岗位人员保密制度和调离制度	6.5 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。
建设运行	制定密码应用方案	7.1 应依据密码相关标准和密码应用需求，制定密码应用方案；
	制定密钥安全管理策略	7.2 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节密钥管理要求参照附录 B；
	制定实施方案	7.3 应按照应用方案实施建设；
	投入运行前进行密码应	7.4 投入运行前应进行密码应用安全

	用安全性评估	性评估，评估通过后系统方可正式运行；
	定期开展密码应用安全性评估及攻防对抗演习	7.5 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。
应急处置	应急策略	8.1 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
	事件处置	8.2 事件发生后，应及时向信息系统主管部门进行报告；
	向有关主管部门上报处置情况	8.3 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

6、评估流程

商用密码应用安全性评估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、分析与报告编制活动。双方之间的沟通与洽谈贯穿整个密码应用安全性评估过程。测评工作流程（包括但不限于）如下图所示。

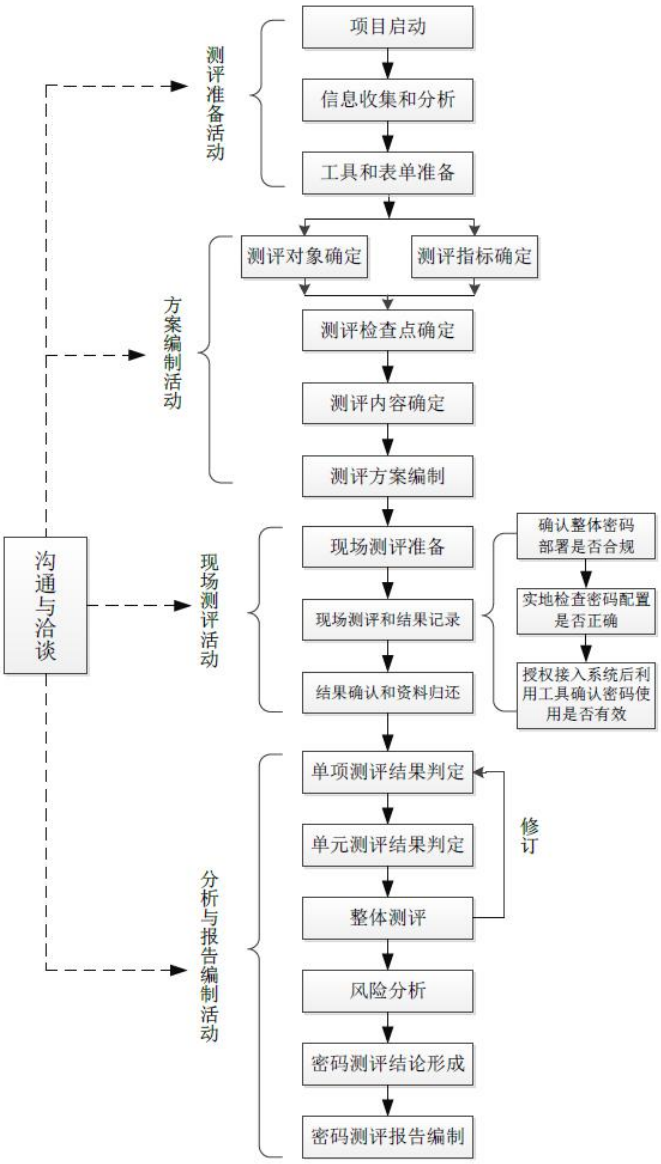

图 1 测评工作流程

7、项目成果

按委托方要求，最终输出被评估系统《密码应用方案评估报告》、《密码应用安全性评估报告》，并协助委托方将评估结果报主管部门及所在地区(部门)密码管理部门备案。

8、组织管理要求

8.1 服务人员

项目组人员通过国家密码管理局商用密码检测中心或国家商用密码应用安全性评估人员测评能力考核小组组织的商用密码应用安全性评估人员测评能力考核.

8.2 验收要求

对每个被测系统出具《密码应用方案评估报告》、《密码应用安全性评估报告》，并协助委托方将评估结果报主管部门及所在地区(部门)密码管理部门备案。