

A 包：

一、服务范围：

1. “好就业”公众服务系统

建设公众服务系统是集就业信息整合、个性化服务推荐、职业指导、技能培训资源匹配及就业成效跟踪于一体的综合性服务平台。它利用大数据、人工智能等先进技术，精准匹配求职者与企业的需求，提供一站式就业服务。求职者可以浏览最新招聘信息，系统智能推荐适合的岗位，并提供职业规划指导，帮助明确职业目标。此外，系统还会对求职者的就业情况进行持续跟踪和评估，包括就业率、满意度等关键指标，为政策制定、企业招聘及求职者提供有价值的参考信息，促进就业市场的供需平衡和良性发展。

2. “好就业”服务管理系统

全面整合公益性、经营性人力资源市场资源，采用“政府搭台、多方参与、劳动者和用人单位受益”的模式，构建“好就业”服务能力。为行业主管部门、人力资源服务机构提供政策管理、企业管理、岗位管理、劳务品牌管理、就业驿站管理、通知公告管理等服务。

通过可视化方式实时展示综合监管仪表盘、就业数据看板、重点群体就业帮扶数据看板、就业数据统计分析等各类信息监测数据。

3. “好就业”数据平台

建设数据底座支撑平台，全面支撑面向未来的就业领域各类数据交换、共享、回流归集、分析、展示、应用和服务，支持就业服务整体情况综合分析、就业失业分析、人力资源服务分析，并按照给定模板生成数据分析报告。数据底座支撑平台是对数据进行治理和数据共享交换的支撑能力，主要以数据标准、数据开发、数据质量与安全、数据资产、数据共享交换为核心开展有效数据管理，使数据中心能够产出高质量、高价值、安全可靠的数据资产，数据治理能力是集数据汇聚、大数据高效处理、数据全流程治理、数据资产管理、数据共享交换于一体，一站式解决数据治理难题，将数据转换为高价值资产，全面提升数据服务能力。

4. 业务协同对接服务

(1) 负责与海南省职业培训信息管理系统、海南省公共就业服务平台、海南省公

共就业服务管理系统、电子档案管理系统、海南省智慧就业监测平台、海南省“好就业”小程序、省数据共享平台、第三方商业平台等系统平台进行对接开发。

- (2) 制定数据对接标准和规范，确保数据传输的准确性、及时性和安全性，实现各系统间就业、人才、社保等相关数据的共享和交换。
- (3) 建立业务协同机制，根据业务流程和需求，优化数据交互流程，保障各系统间业务协同顺畅，为用户提供精准、全面的就业服务，提升市民公共就业服务体验。

二、服务要求：

1. 服务期限

合同签订后 120 日历天内竣工完成并通过验收。

2. 售后服务要求

- (1) 免费质保期：系统在验收后提供 2 年上门免费保修服务。
- (2) 免费质保期内必须提供 7 天×24 小时的电话和网络技术支持服务。
- (3) 系统发生故障后，中标方在 2 小时内远程电话服务支持不能解决问题的，必须在 4 小时内赶到现场，24 小时内排除故障。
- (4) 免费质保期，升级、维修、更换等所需一切支出，由中标方负责。

3. 人员培训要求

中标方必须对系统使用人员进行全面培训，确保系统管理人员能够对系统进行日常管理维护，系统操作人员能够正常使用系统进行各项操作。

4. 免费服务期后系统维护服务要求

对免费服务期结束后应提出升级、更新、维护服务方案，投标人应对服务内容、费用、方式等方面进行承诺。

C包：

一、服务范围：

通过委托专业的网络安全等级保护测评服务机构，依据《信息安全技术网络安全等级保护基本要求》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，服务对象如下：

序号	信息系统/服务项目		级别	备注	服务类型
1	海口市“好就业”精准就业服务平台		三级	S3A3G3	现场服务
2	测评实施过程及结果输出	1. 依据《信息安全技术网络安全等级保护基本要求》等有关管理规范和技术标准，对等级保护对象进行安全等级保护测评； 2. 测评的内容包括安全物理环境、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层面进行合规性检查，分析信息系统与安全保护等级要求之间的差距； 3. 完成测评工作后，《网络安全等级保护测评报告》，并根据信息系统及安全防护措施的现状提出具有针对性的整改意见。			

二、服务要求：

1. 服务期限

采购人下达测评通知书后 60 日内交付测评报告。

2. 服务要求

2.1 服务内容

1) 对用户进行等级保护咨询服务，包括等级保护政策/标准咨询、信息系统等级变更咨询、等级保护建设整改咨询等。

2) 对用户的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统备案工作。

3) 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、安全管理人员、安全管理、安全运维管理等五个方面的安全测评。

4) 完成测评工作后, 提出整改方案; 最后出具符合要求的测评报告。

2.2 项目成果交付

1) 信息系统定级相关文件和报告;

2) 信息系统测评报告及整改建议。

2.3 测评服务步骤

信息系统等级保护测评过程需按照《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。

2.3.1 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
1. 项目启动	1. 组建测评项目组	
	2. 编制《项目计划书》	
	3. 确定测评委托单位应提供的资料	
2. 信息收集分析	1. 定级报告及整改方案分析	《系统基本情况调研表》
	2. 整理调查表单	
	3. 发放调查表单给测评委托单位	
	4. 协助测评委托单位填写调查表	
	5. 收回调查结果	
	6. 分析调查结查	
3. 工具和表单准备	1. 调试测评工具	确定测评工具、形成测评结果记录表
	2. 模拟被测系统搭建测评环境	
	3. 模拟测评	

项目内容	工作内容	成果输出
	4. 准备打印表单	

2.3.2 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
1. 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
2. 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 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	《测评方案》的测评指标部分
3. 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
4. 测试内容确定	识别每个测评对象对象的测评指标 识别每个测评对象对应的每个测试指标的测试方法	《测评方案》的单项测评实施和系统测评实施部分
5. 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 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	《测评方案》的测评实施手册部分
6. 测评方案编制	描述测评项目基本情况和工作依据 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	向用户提交《测评方案》

工作内容	工作详细任务	输出成果
	描述测评对象	
	描述测评内容和方法	

2.3.3 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	向用户确认测评方案
	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. 现场测评和结果记录	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
	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	

工作内容	工作详细任务	输出
		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

2.3.4 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	

工作内容	工作详细任务	工作依据（模版）
	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	

2.4 项目相关要求

项目实施过程中，投标人应遵循国家标准、行业标准。在项目实施中投标人须做到：

- 1) 提供完整的系统实施方案和项目实施管理办法；
- 2) 提供详细的项目实施方案和计划进度说明书；
- 3) 项目实施完成后提供可靠的后期技术服务工作；
- 4) 严格按照双方确定的计划进度保质保量完成工作；
- 5) 规范项目实施过程中的文档管理；
- 6) 有较好的保密管理及风险管理。

D 包：

一、服务范围：

依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》以及国家关于重要领域密码应用的有关要求，通过对海口市“好就业”精准就业服务平台开展密评工作，从物理和环境、网络和通信、设备和计算、应用和数据、安全管理等方面对信息系统开展密码应用安全性评估工作，分析信息系统与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。

项目对象

序号	系统名称	系统等级
1	海口市“好就业”精准就业服务平台	三级

二、服务要求：

1. 服务期限

采购人下达评估通知书后 60 日内交付成果和报告 。

2. 服务内容

本项目包括对海口市“好就业”精准就业服务平台项目进行商用密码应用安全性评估服务，最终输出被评估系统的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	系统评估	依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本	按照 GB/T 39786-2021《信息安全技术 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

序号	服务内容	服务内容子项	工作内容
		要求》等标准进行测评	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。
4	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。

3. 评估内容

针对海口市“好就业”精准就业服务平台项目开展商用密码应用安全性评估，从物理和环境、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，包括但不限于以下内容：

测评单元			测评指标
技术要求	物理和环境安全	身份鉴别	a) 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	b) 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	c) 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	a) 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	b) 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	c) 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	d) 宜采用密码技术保证网络边界访问控制

测评单元			测评指标
		控制信息的完整性	信息的完整性；
		安全接入认证	e) 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	a) 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	b) 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	c) 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	d) 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	e) 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	f) 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	a) 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	b) 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	c) 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；

测评单元			测评指标
		重要数据传输 机密性	d) 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	e) 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	f) 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	g) 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	h) 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 要求	管理 制度	具备密码应用 安全管理制度	a) 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	b) 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	c) 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	d) 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	e) 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	f) 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	了解并遵守密码 相关法律法规	a) 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；

测评单元			测评指标
	管理	规 和密码管理制度	
		建立密码应用 岗位责任制度	b) 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，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任； 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	c) 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	d) 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	e) 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	制定密码应用 方案	a) 应依据密码相关标准和密码应用需求，制定密码应用方案；

测评单元			测评指标
	运行	制定密钥安全管理策略	b) 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, 各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录 A;
		制定实施方案	c) 应按照应用方案实施建设;
		投入运行前进行密码应用安全性评估	d) 投入运行前应进行密码应用安全性评估, 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	e) 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	a) 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	b) 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	c) 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。

4. 项目成果

- 1) 《密码应用安全性评估测评方案》
- 2) 《密码应用安全性评估报告》
- 3) 《密码应用安全性评估整改建议》

5. 服务要求

评估项目实施过程中, 投标人应遵循国家标准、行业标准。

5.1 项目实施要求

在项目实施中投标方必须做到:

- 1) 提供项目实施组织架构;
- 2) 提供详细的项目实施方案和计划进度说明书;
- 3) 严格按照双方确定的计划进度保质保量完成工作;
- 4) 项目实施中要引入风险管理、质量管理;
- 5) 签署《保密协议》。

5.2 项目验收

投标人必须书面通知采购人所完成的工作和准备进行验收的项目种类及验收开始时间,此通知书需经参加联合采购的采购人认定后方可执行。

5.3 验收组织

成立由采购人以及其他有关人员组成的验收小组,负责对项目进行全面的验收。

5.4 验收标准

- 1) 信息系统密码应用安全性评估测评方案;
- 2) 信息系统密码应用安全性评估报告;
- 3) 信息系统商用密码应用安全性评估整改建议;
- 4) 整体性的汇总报告。

6. 服务保障

(1) 投标人必须确保能建立一支具有一定服务能力和管理团队,并合理调配各岗位人员,保障服务工作相关岗位人员需要。

(2) 中标单位在采购人下达评估通知书后 60 日内交付成果和报告

(3) 服务期间提供 7×24 服务响应,技术人员能够在 4 小时之内到达现场,并且现场支持的技术人员具备商用密码应用安全性评估人员测评能力考核证书。

(4) 服务期间提供应急保障工作,针对应急、攻坚克难等事宜提供保障方案,包括高层支撑和响应时间等。

(5) 严守工作秘密。中标服务商必须与采购人签署保密协议,工作人员须与单位签署《保密承诺书》,对知悉的事项及信息予以保密,所有资料、技术文档妥善保管,不得遗失、转借、复印,不得以任何形式向第三方透露;所有密码应用解决方案和采集汇总后的数据严禁通过互联网等公共信息网络、普通邮政进行传递,严禁在连接互联网计算机上存储、处理。

(6) 严格遵循操作规程，承担服务工作质量责任。

E 包：

一、服务范围：

在海口市“好就业”精准就业服务平台建设项目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《测试报告》。

测试对象及范围

序号	系统名称
1	海口市“好就业”精准就业服务平台

二、服务要求：

1. 服务期限

采购人下达测评通知书后 60 日内交付成果和报告。

2. 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》

3. 测试原则

- (1) 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。
- (2) 2、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。
- (3) 3、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。

4. 测评内容应当涉及内容

包括软件功能性、可靠性、易用性、性能效率、信息安全性等质量特性。

- (1) 功能性测试

功能性主要从功能完备性、适合性、准确性 3 个方面内容进行测试。功能性的适合性是必测内容，同时应根据软件特点和用户要求分析准确性、完备性等其他特性的测试需求，确定测试范围和测试内容。

(2) 可靠性测试

可靠性测试主要从成熟性、容错性、易恢复性、可用性等 4 个方面内容进行测试。如果需要，可靠性测试与性能测试结合，测试被测软件的稳定性和健壮性。

(3) 性能效率测试

效率测试主要关注时间特性、资源利用性、容量 3 个方面内容。具体的性能测试场景需要根据具体项目，并现场沟通确定。

(4) 信息安全性测试

信息安全性主要从保密性（产品或系统确保数据只有在被授权时才能被访问的程度）、完整性（系统、产品或组件防止未授权访问，篡改计算机程序或数据的程度）、抗抵赖性（活动或事件发生后可以被证实且不可被否认的程度）、可核查性（实体的活动可以被唯一地追溯到该实体的程度）、真实性（对象或资源的身份标识能够被证实符合其声明的程度）。

1. 项目成果交付

在测试完成后需提供下列技术文档：

- 1) 测试报告；
- 2) 测试问题清单及整改建议；
- 3) 回归测试报告。

F 包：

一、服务范围：

依据CVE（Common Vulnerabilities&Exposures）公共漏洞字典表、OWASP十大Web漏洞（Open Web Application Security Project），以及设备、软件厂商公布的漏洞库，结合专业源代码扫描工具对海口市“好就业”精准就业服务平台进行安全审计。提供包括安全编码规范咨询、源代码安全现状测评、定位源代码中存在的安全漏洞、分析漏洞风险、给出修改建议等一系列服务。

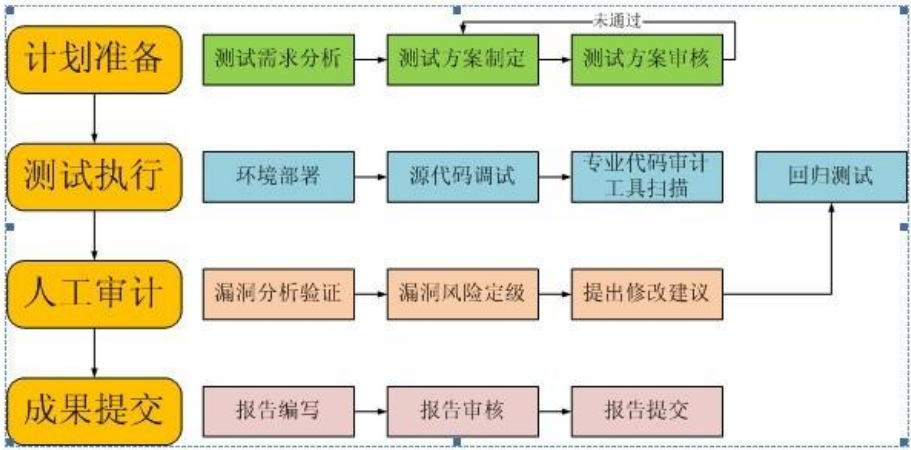
二、服务要求：

1. 服务期限

采购人下达审计通知书后 60 日内交付成果和报告。

2. 服务内容

针对系统开发过程中的编码阶段、测试阶段、交付验收阶段、对各阶段系统源代码进行安全审计检测，利用数据流分析引擎、语义分析引擎、控制流分析引擎等技术，采用专业的源代码安全审计工具对源代码安全问题进行分析和检测并验证，从而对源代码安全漏洞进行定级，给出安全漏洞分析报告等，帮助开发人员统计和分析当前阶段软件安全的风险、趋势，跟踪和定位软件安全漏洞，提供软件安全质量方面的真实状态信息。



3. 服务频率

安全服务提供商提供1次源代码审计服务。

4. 项目成果

《系统源代码代码审计报告》