**4包（**第三方测试及网络安全服务**）**

**一、第三方软件测试需求**

（一）项目概述

为客观公正评估本项目是否满足设计方案的要求，提高信息系统的质量、降低运营风险、减少后期维护成本、保障软件工程质量，现引入第三方测评机构对本项目的功能性、性能效率等质量特性进行专业测评。在系统测评过程中，第三方机构将对软件产品质量进行合理评估，对出现的系统问题，配合应用系统开发单位进行故障定位和优化。提供权威的第三方软件测试报告，对系统建设的质量把关，确保平台建设实现预期建设目标，符合设计需求，符合信息化技术的发展方向，满足业务的应用和开展。

（二）项目目标

完成海南省人力资源开发局业务系统国产化替代改造（2024年）项目的软件测评工作，提供整改建议并协助项目承建方整改，出具测评报告。海南省人力资源开发局业务系统国产化替代改造（2024年）项目建设内容包括：

1.应用系统数据库架构改造升级。

1. 海南省公共就业服务平台就业数智应用系统数据库架构改造；
2. 海南省公共就业服务平台就业数智应用系统数据库迁移。

2.海南省职业培训信息管理系统信创改造及升级。

1. 国产化适配改造；
2. 系统及数据迁移；
3. 系统功能优化升级；

(4)密码应用改造。

（三）服务要求

对本项目开展软件测评服务，对出现的系统问题，配合承建方进行问题定位和优化。并在系统验收前提供权威的软件测评报告。

1.测评标准及规范

（1）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）GB/T 25000.10:2016 《系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第 10 部分:系统与软件质量模型》。

2.测评内容和要求

软件测评对象为本项目开发的应用软件，测评内容包括软件产品的功能性、性能效率用户文档集方面的质量特性。测评人员应以公正、科学、客观、准确的态度，严格按照 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》等国家、国际有关标准规定的检测方法，开展项目软件测评工作。在测评过程中，须及时向采购人及承建单位通报在系统中发现的问题，并于系统测评完成时向采购人提供一份详实的测评报告。如测评中发现要修正的问题，待采购人安排承建方修改完后，要进行回归测评。

本次第三方软件测评服务内容包含以下方面：

（1）功能性测评

功能性测评需要依据需求说明说书和平台建设的有关技术要求，结合用户对系统建设的整体功能方向，对系统涉及到的所有业务逻辑、功能逻辑、功能项等进行全覆盖的测评，及时发现软件系统中存在的问题并提出系统改进意见。

（2）性能效率测评

通过站在用户体验的角度，使用专业的负载生成设备，在性能模型的基础上验证系统是否能够达到用户提出的性能指标，是否符合用户文档中对系统设计时的性能关注点。

（3）用户文档集特性测评

通过用户文档集测试，对系统所属的文档集进行查缺，对单一文档是否可以正确、简明的指引用户对系统的认识、理解、维护的能力进行评价。

（4）易用性测评

①软件系统各项功能应不仅需要明显且正确的显示，确保用户能够准确定位功能，同时还应对于一些特定任务要求的功能，数据应提供响应的提示信息，确保用户能够正确理解。

②易学性方面，除了提供配套的使用手册或文档，以便用户能够查阅并学习系统的使用以外，系统自身还应为用户提供相应的在线帮助功能，达到边用边学的效果。

③对于易操作性相关要求，则应便于用户清楚功能的操作与数据的输入，便于用户快速进行功能的操作与数据的输入，便于用户理解当前的操作状态或结果。

④最需要关注的是系统吸引用户的能力，那么系统应采用统一的界面、统一的菜单、标题、统一的图标和按钮，以及美观的输入框。

3.技术方案

供应商应针对测试范围和测试内容进行分析，制定完整的测试方案，包括但不限于测试策略、测试方法、测试环境等内容。

4.项目实施要求

供应商应针对本项目制定完整的实施方案，包括但不限于进度安排、人力资源计划、质量保证、风险管理、沟通管理等内容。

（1）资源配置

供应商须在其响应文件中清晰陈述对于该项目实施过程中的资源配置情况。包括：

项目的组织结构与职责分工

项目组配备人员的能力与资质

测试环境构建方案

测试工具说明

供应商应在其技术方案中陈述拟安排的资源和可用性保障条件，明确拟投入项目人员的专业背景、项目实践经验、资质及技术能力说明、人员可用性保障说明、测试环境、测试工具可用性保障说明。根据测试的实际需要考虑现场测试，差旅费包含在整体报价中。性能效率测试应采用业界主流的测试工具进行测试，由供应商提供，如果出现知识产权问题，责任归供应商。

（2）工作流程

供应商的技术方案中须清晰描述其如何安排项目实施的工作流程，包含但不限于以下环节：

测试调研：对被测系统进行调研，熟悉测试需求。

测试准备：测试计划、测评方案、测试用例集等的编制和准备。

测试执行：完成实施方案中要求的所有内容，并填写详细测试记录。

测试问题报告提交：提交完整的问题报告。

回归测试：对测试中发现的问题及影响范围进行回归测试。

测试报告提交：提交正式验收测试报告。

（3）质量控制和保障

供应商技术方案中须清晰陈述其对项目实施质量控制和质量保障的方法、控制的目标、内容与流程、项目沟通制度、对于变更的管理等。

（4）项目风险管理

供应商技术方案中须清晰陈述其对项目实施风险管理的方法、以及对项目实施的风险评估和对策，充分考虑项目实施过程风险控制，对可能出现的各种情况有应急预案。

5.服务保密要求

供应商的服务人员均应与采购人签订保密协议。在执行服务过程中应严格按照保密协议相关要求执行。

（四）服务交付物

测试完成后提交相应的测试计划、测试用例及结果、测试报告。

1.服务期及服务地点

服务期：合同签订生效之日起至项目竣工验收为止

服务地点：海南省人力资源开发局

2.验收标准及要求

项目服务完成后，服务成果完全符合采购人需求及合同内容，出具完整的第三方测评报告，项目成果最终通过采购人组织验收。

**二、网络安全服务需求（代码审计、渗透测试）**

（一）项目概述

根据《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)要求，系统上线前需对核心及重要系统的开发交付进行源代码安全检查，防范可能存在的恶意代码、后门程序和安全漏洞。项目涉及的重要系统，参考同业实践经验以及安全管理服务建议，为确保项目建设进度和质量，引入第三方专业服务商开展新线核心及重要系统的源代码安全检查服务。

随着信息技术的快速发展，网络安全问题也日益突出，当前网络安全形势日益严峻，网络攻击和数据泄露事件时有发生，就业数据是国家重要的经济数据，涉及到国家安全和社会稳定。因此，为了保障海南省人力资源开发局业务系统国产化替代改造（2024年）项目网络及数据安全，加强网络安全防护，提高网络安全保障能力成为了迫切的需求。通过委托专业的安全服务机构为海南省人力资源开发局业务系统国产化替代改造（2024年）项目提供网络安全渗透测试服务，可以加强就业数据的安全保障，防止数据泄露和被攻击，协助招标人完成网络安全保障相关事宜。

（二）项目需求

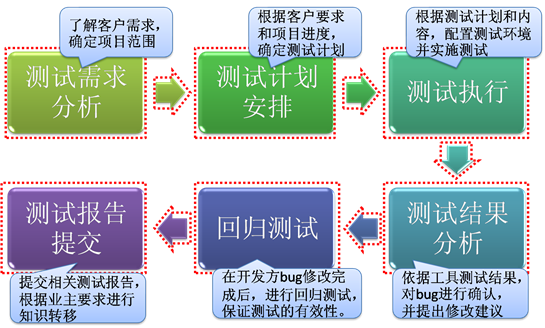
**1.代码审计服务**

网络技术日新月异，以应用系统为核心的信息化进程在不断推进，网络攻击矛头逐步转向各类应用系统。通常情况下，应用系统的安全防护往往依赖于上线前的安全测试和与之关联的外围安全产品所能提供的外在防护，往往忽略了源代码的自身安全，这是导致基于应用系统的安全事件不断涌现的主要原因。据统计，92%的漏洞源自于应用系统，黑客乐此不疲地在不断挖掘和利用着这些漏洞，以期达到各类不可告人的非法目的，许多单位因此蒙受了重大损失，这些漏洞往往是由不安全的编码、不良架构和错误的配置产生的。

代码审计服务的目的在于充分挖掘应用系统代码中存在的安全缺陷及规范性缺陷，从而让开发人员了解其开发的应用系统可能会面临的威胁，并指导开发人员正确修复代码缺陷。将以网络安全等级保护标准规范为基线，由具备丰富编码经验并对安全编码原则及应用安全具有深刻理解的安全服务人员，结合国际化网络安全测试标准，在用户授权许可和安全可控的范围内采用静态分析、动态检测的分析方法，对应用系统源代码和软件架构的安全性、可靠性进行全面的安全检测，发现各类应用系统中存在的安全缺陷和规范性缺陷，从而保障应用系统安全、可靠。

**（1）服务流程**

具体服务流程如下图所示：



**（2）服务内容**

静态代码审计适用于以C、C++、C#、Java等语言开发的应用程序，以及以Ruby、PHP、ASP、JSP、JavaScript和Perl等在内的各种Web技术编写的应用程序，可以是应用程序的全部代码，也可以是一部分完整的代码，只需搭建与用户单位无关的独立的代码分析环境，无需搭建代码运行环境。动态代码审计适用于以Java语言开发的应用程序，需搭建与生产环境类似的功能齐全的应用运行环境（缺失的功能将无法被审计）。源码安全分析人员会使用审计工具和手工分析对程序中的数据流、控制流、语义、结构、配置文件五个层面的脆弱性和安全缺陷进行分析，然后对重点代码进行人工审计。

**审计环境部署：**静态代码审计只需部署分析环境，无需部署代码运行环境，同时需要提供源代码，可进行现场审计，亦可实施异地审计。动态代码审计需提供与生产环境类似的功能齐全的应用运行环境（缺失的功能将无法被审计），以现场审计为主，远程协助为辅；

**静态代码审计：**采用自动静态分析技术扫描某个应用程序的源代码，通过甄别和定位可能存在的薄弱环节数量，以验证该应用程序存在的风险；

**人工验证：**针对审计结果，进行人工验证，剔除误报，客观和全面地发现软件系统自身的安全隐患。

**（2）服务对象及频率**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务内容** | **服务说明** | **服务对象** | **主要成果文档** | **服务类型** |
| 1 | 代码审计服务 | 1. 采用自动静态分析技术扫描某个应用程序的源代码，通过甄别和定位可能存在的薄弱环节数量，以验证该应用程序存在的风险； 2. 对于无法提供源代码的系统，通过在应用程序的字节码中动态插桩检测“探针”，获取应用程序各种运行时的上下文信息，在应用程序运行的同时，实时分析程序的安全弱点； 3. 协针对审计结果，进行人工验证，剔除误报，客观和全面地发现软件系统自身的安全隐患，出具代码审计报告； 4. 在代码风险整改后提供一次审计复核服务。 | 本项目国产化适配及升级改造部分。 | 《应用系统代码审计报告》 | 现场服务 |

**代码审计服务：1次。**

**（3）服务成果**

通过代码审计服务对国产化改造后的信息系统开展代码审计工作，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议，输出包括但不限于《应用系统代码审计报告》。

**2.渗透测试服务**

**（1）服务内容**

渗透测试是一种通过模拟黑客可能使用的攻击方式和漏洞挖掘行为，对目标信息系统的安全进行深入安全检测的一种评估方法。渗透测试的目的是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，从而促进信息系统安全稳定运行。以等级保护测评标准为基线，结合国际化网络安全测试标准，在用户授权下和可控的范围内采取可控的、不造成较大影响的模拟黑客攻击手法，及时发现信息系统的安全漏洞以及没有被掌控到的脆弱点，以便于及时对信息系统存在的安全漏洞及脆弱点进行修复，避免网络安全攻击事件对信息系统造成不良影响。

渗透测试服务的渗透测试指标总共覆盖6个渗透测试层面，24个渗透测试类、137个渗透测试项，渗透测试模拟攻击的目标范围均包括对信息系统中的应用系统、服务器操作系统、数据库系统、网络设备等进行渗透测试。

**（2）服务对象及频率**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务内容** | **服务说明** | **服务对象** | **服务类型** |
| 1 | 渗透测试服务 | 1.渗透测试将覆盖一系列的渗透测试项；  2.渗透测试模拟攻击的目标范围包括信息系统中的应用系统、主机操作系统、数据库系统、网络设备等；  3.提供渗透测试服务，出具渗透测试报告并针对整改进行一次高危风险复核。  渗透测试需要配备专业杀毒工具：  1、无需再终端中安装任何软件或系驱动，即可通过指定位置扫描，快速扫描，全盘扫描对终端设备进行安全检测，可以针对进程扫描、关键未知扫描、开机启动项扫描、系统服务扫描；即插即用无需在目标主机系统上安装任何软件，即可进行恶意软件检测和删除。  2、支持检测感染式病毒、蠕虫、木马、黑客工具、风险软件、灰色软件、垃圾文件、测试文件等6万余家族、1500万余变种的恶意代码。  3、检测文件格式：支持执行文件、文档、媒体文件、图片文件、软件关联格式、脚本、文本格式。  4、复合文件检测：office：rtf，doc，ppt，xls，docx，pptx，xlsx。adobe：pdf，swf。mail：eml，msg，tnef。  5、压缩包检测：支持分析检测种类为58种以上，含压缩包，自解压包，安装包及其他包裹类。  6、恶意文件样本量：支持检测6万余家族、1500万余变种的恶意代码。 | 本项目国产化适配及升级改造部分。 | 远程服务  现场服务 |

**渗透测试服务：2次/年。**

**（3）服务成果**

通过渗透测试服务，模拟入侵者对指定系统进行攻击测试，可以对用户信息平台的安全性得到较深刻的认知，验证经过安全保护后的系统是否真实的达到了预定安全目标。完成渗透测试服务工作后，汇总出具包括但不限于《渗透测试报告》，并提出具有针对性的安全加固建议。

**3.项目服务要求**

**（1）项目实施要求**

**①代码审计服务实施要求**

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：

* 为防止在测试过程中引入恶意代码以及代码泄露，严格选择测试工具，商业工具有专门授权、开源工具进行恶意代码检测后再引入项目。杜绝因工具选择不当造成的将病毒和木马植入的情况发生。
* 代码审计过程中除去自动化审计外，人工审计应当选取适当的策略，保证最大范围覆盖代码所有问题、最大限度的深入挖掘各种漏洞，某些重要工程可以通读代码进行审计。审计之后，在条件允许的情况下尽量在运行环境中进行验证，可以再保证减少误报的情况下挖掘更深层次的问题。；
* 提供完整的系统实施方案和项目实施管理办法；
* 提供详细的项目实施方案和计划进度说明书；
* 项目实施完成后提供可靠的后期技术服务工作；
* 严格按照双方确定的计划进度保质保量完成工作；
* 规范项目实施过程中的文档管理；
* 承诺与招标方签订保密协议，同时公司与每个参与本项目的员工就本项目签订信息保密协议，并承诺严格遵守保密协议中规定的要求。

**②渗透测试服务实施要求**

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：

* 提供完整的系统实施方案和项目实施管理办法；
* 项目实施完成后提供可靠的后期技术服务工作；
* 严格按照双方确定的计划进度保质保量完成工作；
* 规范项目实施过程中的文档管理。

**2（2）项目验收要求**

中标人必须提供给业主详细的项目验收方案。

**验收组织：**

成立由业主、中标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。

**验收标准：**

标准化：项目验收最关键的指标，应确保测评过程符合国家标准规范；

系统稳定性：在测评过程中应确保软硬件环境的稳定性、运行正常；

系统文档：验收文档是否齐全、规范、准确、详细；

系统可操作性：交付成果清晰、通俗易懂。

（三）售后服务保障与承诺

1.代码审计服务售后服务保障与承诺

对于服务中发现的应用系统代码缺陷，投标方应提供项目验收后一年内的跟踪服务，对本次服务范围内的问题提供远程或现场技术咨询，对于缺陷的修复、问题的排除给出建议和指导。

2.渗透测试服务售后服务保障与承诺

对于现状测试过程中发现的安全问题，投标人应先出具问题汇总报告，并给招标人预留二十天的整改时间，整改完成后投标人提供一次全面问题复查，出具包括但不限于《渗透测试报告》。