第三章 采购需求

B包：海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）监理服务（第二次采购）

一.监理服务要求

项目建设内容

监理内容为海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目的全部建设内容。

二、监理服务内容

监理工作依据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57号）等国家法律、法规、行业标准，以及政策要求，和《信息化工程监理规范》，落实“网络安全三同步一评估”，对本项目海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目建设内容进行包括项目实施和验收阶段的全过程监理工作。采用“四控三管一协调”的监理方式，对项目进行质量、进度、投资、变更的全面控制和监督，负责相关的合同管理、信息管理、知识产权管理，负责上述整个项目全过程监督协调，从而使本工程“按期保质、高效、节约”地完成。

三、监理服务要求

1.工程实施阶段要求

监理单位应依据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57号）等国家法律、法规、行业标准，以及政策要求，加强项目实施

方案审核，促使项目中所使用的产品和服务符合委托合同及国家相关法律、法规和标准；明确项目实施计划，对于计划的调整应合理、受控；促使项目实施过程满足委托合同的要求，并与项目设计方案、项目计划相符。监理单位应完成（包括但不限于）如下工作：

1)项目实施前，监理单位应提供熟悉应用软件、网络安全、密码安全的技术人员，全程参与本项目的现场勘察和调研，并对承建单位提供的详细设计、实施方案、工程图纸、施工工艺、造价清单等资料进行核查，对其缺陷、遗漏、工作边界等进行评审，及时与建设单位汇报工作成果，并出具监理评审意见。

2)项目实施前，监理单位应审核承建单位提交的质量管理计划、项目实施计划，审核后签署监理审核意见；

3)项目实施前，监理单位应组织建设单位、承建单位召开项目实施启动会，要求承建单位落实实施计划、实施方案和必要的准备工作，会议内容做会议纪要，并经三方签认；

4)项目实施前，监理单位应审核承建单位提交的项目实施方案，审核后签署监理意见。

5)监理单位应审核承建单位提交的开工申请，检查项目准备情况。项目实施条件具备时，总监理工程师应签发开工令，并报建设单位开始项目实施；

6)监理单位应监督合同执行情况，通过监理周报、月报、阶段性报告定期向建设单位提交监理报告，跟踪项目的质量、进度、投资完成情况；

7)监理单位应对项目质量进行全过程监督管理，在加强现场管理工作的前提下对重要部位和关键点应采取“旁站监理”的方式，检查项目进度和质量，做好隐蔽工程的签证；提供具有专业技术能力的技术人员对项目建设中涉及的网络安全、应用密码建设等内容进行核查，对发现的可能影响质量的问题及时指令承建

单位采取措施解决，必要时发出停工、返工的指令，并及时书面告知建设单位；

8)监理单位做好监理日志，随时记录实施中有关质量、进度等方面的问题，并对发生质量问题的现场及时拍照或录相；

9)监理单位组织对承建单位提供的产品及服务进行验收，对验收结果做验收记录，并经三方签认；对不符合合同或相关标准规定的产品及服务应拒绝签认。没有被签认的产品及服务不得在项目实施中应用；

10)监理单位应检查设备到货安装环境；监督旁站设备到货、安装、调试过程。监督软硬件平台集成过程。必要时，监理单位据委托合同、技术标准或事先约定的方法检测产品及服务的质量，对于数量较大的同类型产品及服务，监理单位可采取抽样方法；

11)必要时，监理单位应要求承建单位提交第三方测试机构出具的测试报告，并核验产品认证证书、检测报告的真实性、有效性；第三方测试机构应经建设单位和监理单位同意；

12)监理单位应按计划检查承建单位项目实施状况、人员与实施方案的一致性；

13)监理单位应执行已确定的阶段性质量监督、控制措施及方法，并做监理日志。出现项目质量问题时，经确认后监理机构签发监理通知单，报建设单位、承建单位，责令承建单位整改；

14)监理单位应及时处理承建单位提交的项目中关键环节的实施申请，审核其合理性后签认，报建设单位批准；必要时，监理机构应检查承建单位重要项目步骤的衔接工作，做监理日志。未经监理工程师检查认可，承建单位不能进行与之相关的下一步骤的实施；

15)建设单位或承建单位提出的工程变更，监理单位根据实际情况，收集相

关数据或信息，参考设计文件及其它有关资料，按照承建合同的有关条款，对工程变更范围、内容、实施难度以及变更的投资和工期做出评估，并出具监理评审意见，涉及应用系统软件的需求或设计变更，还应提供《软件造价评估报告》以保证对建设投资的管理；

16)监理单位应及时处理工程变更申请，审核变更的合理性，保证项目总体质量不受影响;监理机构应从目标系统的质量、进度和投资等方面审查工程变更，由于变更引起投资的改变应按照合同的相关条款执行。在合同中没有规定的，应在变更实施前与建设单位、承建单位协商确定变更导致的投资变化，并作工程备忘录；

17)监理单位对工程变更过程及结果形成书面记录，确保变更过程规范、可追溯。同时要求在变更文件签署前，监理单位不得单方批准承建单位实施工程变更；

18)当出现项目事故时，监理单位应要求承建单位在事故发生后立即采取措施，尽可能控制其影响范围，并及时签发停工令，报建设单位，并与建设单位、承建单位共同确认初步处理意见；监理单位应监督承建单位采取措施，查清事故原因，审核承建单位提出的事故解决方案及预防措施，提出监理意见，提交建设单位签认；监理单位应审查承建单位报送的事故报告及复工申请，条件具备时签发复工令；

19)监理单位若发现项目实施过程存在重大质量隐患，应及时向承建单位签发停工令，并报建设单位，监督承建单位进行整改。整改完毕后，及时处理承建单位的复工申请；

20)监理单位应根据项目总进度计划，编制控制性总进度计划，并协助建设单位编制总体进度计划或实施总进度计划；审批实施总进度计划以及分年的年、

季、月计划；跟踪监督、检查、记录进度计划的实施；对实际进度进行对比、检查、分析，对出现的偏差采取应对措施；审查承建单位的进度报告，并编报监理报告；

21)监理单位应对项目实际进度做好记录和统计工作，并进行经常性和阶段性的项目实际进度与计划进度的对比分析，检查进度偏差的程度和产生的原因，分析预测进度偏差对后续实施工序和项目的影响程度，并提出指导性的解决措施。当项目实际进度与计划进度相比发生较大偏差而有可能影响合同工期目标的实现时，监理单位应提出进度计划的调整意见，并指导承建单位相应调整进度计划。进度计划的重大调整应书面报建设单位批准；

22)监理单位应依据委托合同及其补充协议，审核承建单位提交的项目阶段性报告和付款申请签发工程款支付意见，报建设单位签认；

23)监理单位应对项目实施阶段三方共同参与的过程和活动做工程备忘录；并检查督促承建单位按规程规范实施、文明安全实施，防止因出现质量、安全事故及环保问题

24)监理单位应根据需要及时组织专题会议，解决项目实施过程中的各种专项问题，并做会议纪要，提交建设单位和承建单位。

25）依据国家保密法律法规，根据工程的具体情况，协助建设单位划定保密范围和保密内容，并制定相应的保密措施和保密控制流程，做好工程资料的安全保密管理工作，严格控制接触涉密资料的人员范围。

26）根据国家网络安全法，由项目网络安全需要满足公安机关的信息安全等级保护要求，为了加强项目建设过程的网络安全等级保护工作，确保系统建成后通过信息安全等级保护测评，监理单位还应该提供下列服务：

在项目前期阶段，根据《信息安全技术网络安全等级保护基本要求》

（GB/TGBT22239-2019），辅助业主对项目的网络安全建设方案进行评审、论证。

在项目验收阶段，按照《信息安全技术网络安全等级保护基本要求》（GB/TGBT22239-2019），为业主提供包括安全策略、管理制度、操作规程等管理要求的咨询服务。

2.工程验收阶段要求

监理单位应评审项目测试验收方案（验收目标、责任双方、验收提交清单、验收标准、验收方式、验收环境等）的符合性及可行性；促使项目的最终功能和性能符合委托合同、法律、法规和标准的要求；推动承建单位所提供的项目各阶段形成的技术、管理文档的内容和种类符合相关标准。合同验收时监理单位应完成（包括但不限于）如下工作：

1）依据《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57 号）以及本项目建设需求和合同中约定的各项要求，检查与测试是确认项目各系统所建内容是否达到合同要求和评估系统质量的必备措施，监理单位应协助建设单位明确项目测试验收方案并审查其符合性及可行性。

2）监理单位应及时处理承建单位提交的验收申请，审核竣工结算，审核验收的必备条件，并签署监理意见；

3)监理单位应协助建设单位对验收中发现的质量问题进行评估，根据质量问题的性质和影响范围，敦促承建单位根据验收整改要求提出整改方案，并监督整改过程。必要时，应组织重新验收；

4)监理单位应督促承建单位完成项目实施方案中确定的培训，并对培训效果做出评估；

5)监理单位应协助建设单位进行工程决算；

6)监理单位应敦促建设单位、承建单位按照事先约定，编制、签署和妥善保

存验收阶段的项目文档；

7)监理单位应编写各时段项目验收的监理工作报告，整理监理单位应提交和提供的验收资料；负责整理记录归档建设单位与承建单位来往的文件、合同、协议及会议记录等各种文档，出具监理文件。

8)督促承建单位做好售后服务，分别审核并落实质保期的质量保障，并建立应急响应制度和流程，为后续开展等保测评工作提供必要的技术和服务支撑。

9)监理机构应协助建设单位和承建单位完成项目移交工作，将项目移交建设单位管理，并进入工程质量保修期。

四、服务团队要求

1.参与本项目的监理团队（含总监理工程师）不得少于 5 人，且需全部具有人力资源和社会保障厅（局）颁发的《信息系统监理师》证书；

2.本项目实行总监理工程师负责制，应具备信息系统项目管理师、软件测试工程师、软件设计工程师、咨询工程师等相关证书，对信息系统建设有全面了解；对国家网络安全法、密码法等法律法规、行业标准有充分理解，具有丰富的实施项目管理、咨询、检测和沟通协调能力，具有预见和应对项目风险能力；

4.参与本项目的监理人员需提供近六个月的社保缴费证明，同时，保证监理人员的稳定性，监理工作开始后，原则上不允许更换监理工程师，如要更换，须经建设单位同意。

（2）商务要求

1、服务期限、服务地点和服务方式（履约时间、地点和方式）：

1.1 合同履行期限（服务期）：本项目监理服务周期自签订合同之日起至建设项目完成竣工验收。

1.2 服务地点（履约地点）：用户指定地点

1.3 服务方式（履约方式）：按本招标文件要求和中标人投标文件的规定

2、付款时间、方式及条件：（具体以实际签署合同为准）

（1）合同签订之日起 10 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 40%；（2）项目初验合格并上线试运行后 10 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 30%；（3）项目通过整体竣工验收完成后 10 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 30%。

3、知识产权要求：

投标人应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其他知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。

4、其他：

4.1、项目的实质性要求：按本招标文件要求和中标人投标文件的规定。

D包：海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）网络安全服务（第二次采购）

一、网络安全服务需求

1、渗透测试服务

在项目建设单位授权范围内，参考OWASP标准（渗透测试执行标准）对海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目进行模拟黑客攻击服务，用于帮助项目建设单位评估海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目当前的安全性。提供测试包括外网渗透测试、内网渗透测试、黑盒测试、灰盒测试等，覆盖系统中包含的服务器、数据库、中间件、网络设备等相关软硬件资产。

服务对象

海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目

服务内容

渗透测试作为检验目标系统安全性最有效的服务，需要安全服务人员通过专用工具扫描与人工测试、分析的手段，以模拟黑客入侵的方式对海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目进行模拟入侵测试，主要评估海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目是否存在SQL注入、跨站脚本、跨站伪造请求、认证会话管理、弱口令、信息加密性、文件包含、目录浏览、不安全的跳转、溢出、上传、不安全的数据传输、未授权的访问等脆弱性问题，识别服务目标存在的安全风险。

服务标准

1)、采用人工黑盒的方式对业务系统的应用系统进行模拟攻击测试。主要测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web脚本渗透、B/S或C/S应用程序测试等；

2)、测试应包含WEB安全类，包括：SQL注入、跨站脚本攻击（XSS）、XML外部实体（XXE）注入、跨站点伪造请求（CSRF）、服务器端请求伪造（SSRF）、任意文件上传、任意文件下载或读取、任意目录遍历等测试项。

3)、测试应包含业务逻辑安全类，包括：用户名枚举、用户密码枚举、用户弱口令、会话标志固定攻击、平行越权访问、垂直越权访问、未授权访问、验证

码缺陷等等测试项；

4)、测试应包含中间件安全类，包括：中间件配置缺陷、中间件弱口令、WEBLOIGC 反序列化命令执行、JBOSS 反序列化命令执行、WEBSPHERE 反序列化命令执行等测试项。

5)、测试应包含服务器安全类，包括：域传送漏洞、REDIS 未授权访问、MANGODB 未授权访问、操作系统弱口令、数据库弱口令等测试项。

6)、服务应包含安全整改指导以及复查测试。

服务成果：

完成渗透测试工作后，出具《渗透测试报告》，并提出具有针对性的安全加固建议。

2、代码审计服务

在海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目正式上线前，完成 1 次代码审计服务服务。

服务对象

海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目。

服务标准

（一）审计目的

针对海南国际贸易“单一窗口”（海南自贸港物码溯源管理系统）项目的应用系统的核心代码，通过代码审计服务，以发现程序错误，安全漏洞和违反程序规范为目标对编程项目中源代码的进行全面分析，对应用系统进行白盒安全检测。通过对系统开发框架、应用程序、客户端程序、接口及第三方组件和应用配置这五个方面进行深入的安全分析，充分挖掘当前源代码中存在的安全缺陷以及规范性缺陷，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程序缺陷。

（二）服务标准和规范

(1)GB/T 34943-2017《 C/C++语言源代码漏洞测试规范》

(2)GB/T 34946-2017《 C#语言源代码漏洞测试规范》

(3)GB/T 34944-2017《 Java 语言源代码漏洞测试规范》

(4)SJ/T 11682-2017《C/C++语言源代码缺陷控制与测试指南》

(5)SJ/T 11681-2017《C#语言源代码缺陷控制与测试指南》

(6)SJ/T 11683-2017《JAVA 语言源代码缺陷控制与测试指南》

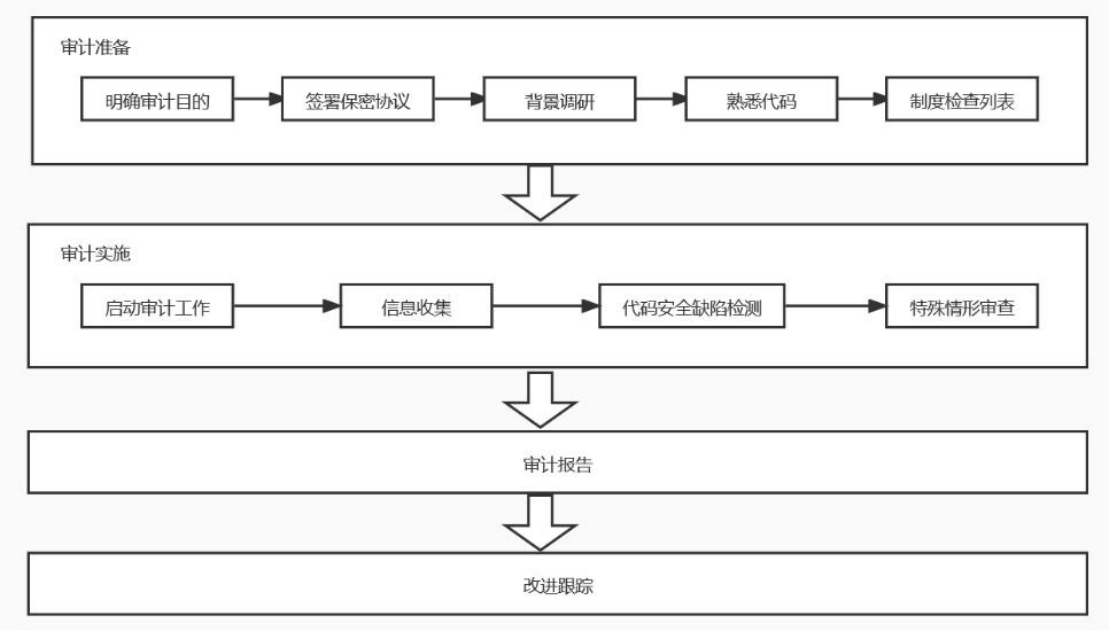
(7)GB/T 39412-2020《信息安全技术 代码安全审计规范》

(8)GB/T 20984-2007《信息安全技术 信息安全风险评估规范》

(9)GB/T 22081-2016《信息技术 安全技术 信息安全控制实践指南》

(10)GB/T 31509-2015《信息安全技术 信息安全风险评估实施指南》

（三）审计流程



（四）审计服务内容

通过源代码检测针对重要信息系统的软件代码进行问题检测，包括对配置错误、边界条件错误、访问验证错误、意外情况处理失败、策略错误、来源验证错误、跨站脚本、修改参数提交、修改隐藏值、Cookie 欺骗、SQL 注入攻击、习惯问题、使用错误等各个问题点进行逐一排查，以发现是否有恶意代码、木马挂马、恶意的嫌疑行为（使用了 LSP 等劫持技术，监控或截取了键盘、显示、网络等设备，使用了插件，有用户不知情情况下的自动行为等，并指导进行安全整改及复测检查。

（五）服务对象

代码审计服务主要对象包括并不限于对 Windows 和 Linux 系统环境下的以下语言进行审核：java、C 语言、C#、ASP、PHP、JSP、.NET 全面测试。

（六）成果交付

在完成代码审计后需提供下列技术文档：

1)、问题清单及整改建议；

2)、《海南省 XX 单位 XX 系统源代码代码审计报告》。

3、安全风险评估服务:

投标人应根据《信息安全技术 信息安全风险评估规范》(GB/T 20984-2007)、《信息安全技术 信息系统安全保障评估框架》(GB/T 20274-2008）等国家风险评估工作相关规范和标准，对海南国际贸易“单一窗口”(海南自贸港物码溯源管理系统）项目网络安全进行风险评估工作。包括风险评估准备、资产识别、威胁识别、脆弱性识别、风险分析以及风险评估文件记录。

服务对象

海南国际贸易“单一窗口”(海南自贸港物码溯源管理系统）项目。

服务内容

1) 风险计算：在完成资产识别、威胁识别、脆弱性识别以及对已有安全措施确认后，投标人应采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险。

2) 风险结果判定：为实现对风险的控制与管理，可以对风险评估的结果进行等级化处理。投标人应根据所采用的风险计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表相应风险的严重程度。

3) 风险处理计划:对不可接受的风险投标人应根据导致该风险的脆弱性制定风险处理计划。风险处理计划中明确应采取的弥补弱点的安全措施、预期效果、实施条件、进度安排、责任部门等。安全措施的选择应从管理与技术两个方面考虑。安全措施的选择与实施应参照信息安全的相关标准进行。

4) 残余风险评估:在对于不可接受的风险选择适当安全措施后，为确保安全措施的有效性，投标人应进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。残余风险的评估可以依据本标准提出的风险评估流程实施，也可做适当裁减。一般来说，安全措施的实施是以减少脆弱性或降低安全事

件发生可能性为目标的，因此，残余风险的评估可以从脆弱性评估开始，在对照安全措施实施前后的脆弱性状况后，再次计算风险值的大小。

服务成果

完成风险评估服务工作后，提交《信息安全风险评估文档》。

二、商务要求

1、服务期限、服务地点和服务方式（履约时间、地点和方式）：

1.1 合同履行期限（服务期）：采购人下达测评通知书后 60 日内交付成果和报告。

1.2 服务地点（履约地点）：用户指定地点

1.3 服务方式（履约方式）：按本招标文件要求和中标人投标文件的规定

2、付款时间、方式及条件：（具体以实际签署合同为准）

（1）本合同签订后，甲方收到乙方开具的增值税普通发票 10 个工作日内向乙方支付合同金额的 50% ；（2）乙方履行完毕本合同规定的技术服务后，甲方收到评估报告并确认报告完整、准确并通过大数据局组织终验通过，甲方收到乙方开具的增值税普通发票 10 个工作日内向乙方支付合同金额剩余的 50%。

3、知识产权要求：

投标人应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其他知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。

4、投标人须针对以下要求进行响应，提供承诺函，加盖公章：

4.1、服务周期内提供重大活动和节假日现场保障服务。

4.2、项目实施完成后提供可靠的安全培训服务工作；

4.3、严格按照双方确定的计划进度保质保量完成工作；

4.4、提供 2 年免费运维期内的持续保障服务。

5、其他：

5.1、项目的实质性要求：按本招标文件要求和中标人投标文件的规定。