

采购需求

一、项目概况

依据《中共中央办公厅 国务院办公厅印发关于推进社会信用体系建设高质量发展促进形成新发展格局的意见》提出“（十五）健全信用基础设施。统筹推进公共信用信息系统建设。加快信用信息共享步伐，构建形成覆盖全部信用主体、所有信用信息类别、全国所有区域的信用信息网络，建立标准统一、权威准确的信用档案。”的要求，按照《智慧海南总体方案（2020-2025年）》、《海南省社会信用体系“十四五”规划》的“打造全面信用信息共享融合内核，实现面向法人、非法人组织和自然人信用信息和信用综合服务全覆盖，信用信息丰富度显著提升”的工作任务，以及《海南省社会信用体系建设联席会议工作办公室关于印发沈晓明书记“揭榜挂帅”项目2022年重点工作任务的通知》中提出的“强化信息系统支撑能力”的工作部署，建设全国信用信息共享平台（海南儋州）二期。即，以公共信用信息平台为枢纽，实现与省级平台以及全市各级部门信用信息的常态化归集、交换、共享，构建完善全市范围内的法人信用信息、自然人信用信息数据库；建成数据处理高效高质、共享交换及时畅通、信息融合增值增效、信息服务灵活适用、运维体系安全可靠的新一代信用系统；以公共信用信息平台为载体，借鉴城市信用监测排名靠前的城市经验和做法，依托公共信用信息平台开展常态化的业务工作和应用服务，进一步推进儋州信用体系建设，提升儋州城市信用监测排名，进一步推进“诚信儋州”建设，深入推进“放管服”改革，更好地发挥信用在提高市场监管能力、激发市场活力、提升社会治理水平、优化营商环境的基础性作用，为优化营商环境和实现高质量发展提供支撑。

通过全国信用信息共享平台（海南儋州）二期建设，能够促进儋州市各类信用主体的信用状况公开透明、可查可核，实现多部门、跨地域、跨领域信息联享、信用监管、守信联奖、失信联惩的共享机制，使守信者一路绿灯、失信者处处受限，提升儋州市信用体系“软实力”和“硬支撑”，有利于建立以信用为核心的新型监管和社会治理方式，推动社会信用体系建设向纵深发展。

二、采购项目预（概）算

总 预 算：2881107.43 元

包 A（信用平台二期项目）预算：¥2494038.94 元

包 B（监理服务）预算：¥71737.69 元

包 C（软件测评） 预算：¥55330.80 元

包 D（网络安全等级保护测评） 预算：¥80000.00 元

包 E（商用密码应用安全性评估）预算：¥120000.00 元

包 F（软件代码检测服务）预算：¥60000.00 元

三、技术商务要求

1. A 包：信用平台二期项目

（1）技术要求如下：

一、本期项目建设内容

1、升级改造信用网站

根据国家平台和网站一体化的要求，在二期基础上升级改造网站栏目板块、内容管理和发布、信用信息查询、信用信息公示、网站系统管理功能；新建信用承诺公示、信用自主申报、“信易+”服务、异议投诉申请、信用修复申请等功能，丰富信用信息展示与查询内容。

2、升级改造信用信息共享平台建设

按照国家最新城市信用监测及信用示范城市要求，在二期基础上升级改造数据管理系统、数据采集系统、数据交换系统，新建数据处理系统、数据质量保障管理、数据监控系统等。通过信用信息共享平台全面增强我市信用信息的汇聚融合能力、价值发现能力、开放共享能力、应用服务能力，信用信息资源管理体系和服务体系全面升级，信用信息作为海南自由贸易试验区基础性战略资源的作用更加突出，为更好服务海南自由贸易港建设并融入新发展格局、打造高标准的市场体系、营造法治化、国际化、便利化的营商环境、构建以信用为基础的新型监管机制和公共信用信息应用服务体系提供强有力支撑。

3、信用联合奖惩系统

本期新增信用联合惩戒系统，通过备忘录管理、奖惩对象管理、奖惩协同执

行、奖惩结果反馈以及联合奖惩信息应用服务等模块，建立完善的守信联合激励和失信联合惩戒机制，实现守信联合激励与失信联合惩戒认定、启动、推送、接收、执行、反馈、形成报告的工作闭环管理机制，建立对激励或惩戒过程、激励或惩戒方式、激励或惩戒结果等的整体管理，实现一处触发、处处响应的信用奖惩联动功能，推动各级已发布的联合奖惩措施落实落地。

4、“双公示”等行政权力事项管理系统

本期新增“双公示”等行政权力事项管理系统，通过归集处理、数据监测、督办管理、考核管理、工作台五大功能模块，落实对各数据项所要求的校验规则，通过信息归集和处理，实现“双公示”及五类行政管理信息的精细化管理。

5、信用信息分析系统

本期新增信用信息分析系统，通过信用工作一页清、信用主体画像和信用主体关联分析功能模块，对黑名单、行政处罚等高频信用信息的使用情况分析展示，实现各部门信用管理者对信用工作开展各项情况的一屏掌握、一屏尽览。提高信用工作的分析研判、辅助决策、汇报展示等能力。

6、信用承诺管理系统

本期新增信用承诺管理系统，通过信用承诺数据归集、信用承诺监察、信用承诺分析预警和信用承诺服务等模块，支撑信用承诺信息、信用践诺信息的归集、处理、分析、预警、核查、服务等工作机制，支撑承诺践诺信息全省统一的规范化管理与应用，实现自动化的信用监测与信用预警。

7、信用分级分类监管系统

本期新增信用分级分类监管系统，通过分级分类监管事项清单管理、信用监管留痕管理、信用监管专题分析和信用监管综合分析等功能模块，归集各重点领域行业信用监管数据，结合公共信用信息构建各重点领域行业分级分类监管主题库，实现全市各重点领域分级分类信用监管事项的标准化、规范化、精细化管理，提高监管能力和分析能力。

8、政务诚信管理系统

本期新增政务诚信管理系统，通过政务诚信目录管理、政务诚信主题库、政务诚信教育管理、重点领域政务诚信监管和政务领域信用档案管理五大功能模块，实现政务信用信息归集、交换和整合，构建政府部门和公务员政务领域信用主题

库，提升对失信政府部门和公务员的信用监管。

9、合同履行管理系统

本期新增合同履行管理系统，通过合同目录清单管理、合同履行归集管理、合同履行自主申报、合同履行信息处理、合同履行信息跟踪分析以及合同履行信息公示功能模块，对相关合同的签约、履约、违约信息进行标准化处置和分析，对合同履行全流程情况进行跟踪、预警、处置、评价等处理；为政府部门和金融服务机构在企业项目审批、政策扶持、融资授信等方面提供信息支撑。

10、公共信用服务系统

本期新增公共信用服务系统，通过信用修复系统和异议处理系统功能模块，提供信用信息异议的申请发起、收件、审核、办理和反馈全流程管理，实现信用修复的发起、收件、审核、办理和反馈全流程管理。

11、“信易+”应用管理系统

结合儋州特点、产业优势，本期新增“信易+”应用管理系统，通过“信易批”、“信易租”和“信用+港口监管”三大功能模块，开展“信易+”守信激励工作，扩大“信易+”应用场景，丰富守信激励内容，向符合支持条件的诚信主体提供优质高效的“信易+”服务。在“信用+港口监管”方面，针对港口行业的特点，基于企业信用数据支撑部门精准开展信用监管工作，提供信用查询、信用公示、风险预警、事中事后信用监管等功能。

12、与省发改委省级信用平台信息共享对接

本期项目需与海南自由贸易试验区信用信息共享平台进行数据共享交换，实现信用信息的数据交换互补。包括社会法人、自然人的行政许可数据和行政处罚数据，归集红黑名单数据。

二、系统功能需求

1、升级改造信用网站

信用中国（海南儋州）作为我市社会信用体系建设的总窗口，按照国务院办公厅关于印发政府网站发展指引的通知、国家发展改革委关于加强全国信用门户网站一体化建设的要求，充分借鉴获得“全国信用信息共享平台和信用门户网站一体化建设示范性平台和网站奖”的先进省市信用平台成果，在一期项目建设的基础上升级改造信用网站，面向社会公众用户、实名制用户提供信用信息发布、

信用信息公示、信用信息一站式关联查询、信用应用服务、信用宣传等栏目。

系统功能主要包括：网站栏目板块、内容管理和发布、信用信息查询、信用信息公示、信用承诺公示、信用自主申报、“信易+”服务、异议投诉申请、信用修复申请、网站系统管理等。

2、升级改造信用信息共享平台

依据国家发展改革委关于加强全国信用信息共享平台一体化建设的要求，在第一期项目建设的基础上梳理最新版本的全国公共信用信息基础目录，优化公共信用信息资源管控与服务能力，完善信用信息归集，将信用信息变为有价值的资产，打破“信息孤岛”。

按照统一的数据接口标准和规范，升级改造信用信息共享平台，建立信用数据标准体系和多层次开放式数据接口，继续扩大法人和自然人信用信息归集范围，汇集整合各行政机关、司法机关、金融机构、公共事业单位及相关组织掌握的各类法人信用信息和自然人信用信息，实现跨部门信用信息的汇集、交换、处理和共享，建成法人信用数据库和自然人信用数据库，并提供数据全生命周期过的监控、配置、统计和管理；推进平台与国家、海南省信用平台的信息交换和共享。

本期升级改造系统功能主要包括：数据采集系统、数据交换系统、数据处理系统、数据管理系统、数据质量保障管理、数据监控系统等。

3、信用联合奖惩系统

依据《海南省优化营商环境行动计划（2018-2019年）》，利用儋州市信用信息共享平台对接海南审批一张网，实现各部门各单位审批服务的互联互通和信息共享，通过数据比对、信息共享、信用报告等方式提供信用信息支撑，协助实现企业办理简单事项、经常办理事项以及可共享实现的事项“一次都不用跑”，办理复杂事项“最多跑一次”。

联合惩戒服务系统主要是建立完善的守信联合激励和失信联合惩戒机制，加快推进社会诚信建设，加强各单位信用信息公开和共享。实现守信联合激励与失信联合惩戒认定、启动、推送、接收、执行、反馈、形成报告的工作闭环管理机制，建立对激励或惩戒过程、激励或惩戒方式、激励或惩戒结果等的整体管理，可在系统中对每个节点进行查看、审核与监督，确保惩戒工作在每个环节的透明度，方便各部门在政务审批时对信用主体进行信用前置核查。实现一处触发、处

处响应的信用奖惩联动功能，推动各级已发布的联合奖惩措施落实落地。

系统功能主要包括：备忘录管理、奖惩对象管理、奖惩协同执行、奖惩结果反馈、联合奖惩信息应用服务等。

4、“双公示”等行政权力事项管理系统

依据国家发改委新版“双公示”及五类行政管理信息（行政强制、行政确认、行政裁决、行政奖励和行政监督检查）要求，系统落实对各数据项所要求的校验规则，实现信息归集和处理；依据国家对“双公示”及五类行政管理信息的考核指标，实现“双公示”及五类行政管理信息的精细化管理。

系统功能主要包括：归集处理、数据监测、督办管理、考核管理、管理工作台等。

5、信用信息分析系统

通过直观的报表和图形化手段，实现各部门信用管理者对信用工作开展各项情况的一屏掌握、一屏尽览，对黑名单、行政处罚等高频信用信息的使用情况分析与展示，适应我市社会信用体系建设对信用工作日常管理、分析研判、辅助决策、汇报展示、业务观摩等多样化的应用场景的展示需要。

系统功能主要包括：信用工作一页清、信用主体画像、信用主体关联分析等。

6、信用承诺管理系统

支撑信用承诺信息、信用践诺信息的归集、处理、分析、预警、核查、服务等工作机制；实现信用主体的在线承诺；拓宽数据归集渠道，完成信用主体承诺、践诺情况的多源数据汇聚；提供信用承诺核查接口；支撑承诺践诺信息全省统一的规范化管理与应用，实现自动化的信用监测与信用预警，为信用监管和告知承诺制改革提供支撑。

系统功能主要包括：信用承诺模板管理、信用承诺数据归集、信用承诺服务、信用承诺监察、信用承诺分析预警、信用承诺信息统计分析等。

7、信用分级分类监管系统

按照《国务院办公厅关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》要求，加快推进将信用信息和信用审查报告嵌入到行政管理和公共服务的各领域、各环节，应用到政务服务一张网中，作为行政管理和政务服务的事中事后监管重要信用应用，在生态环境、工程建设、市场监管、食

品安全、司法公信和金融信贷等领域寻求突破，推动构建信用监管联动机制。

对信用监管事项进行目录清单式的标准化管理，实现分级分类信息的精准化推送，支撑信用监管业务的跨部门协同，实现信用监管业务的执行反馈。归集各重点领域行业信用监管数据，结合公共信用信息构建各重点领域行业分级分类监管主题库；实现全市各重点领域分级分类信用监管事项的标准化管理，获取分级分类监管的监管对象清单和监管结果反馈数据，对各重点领域行业分级分类监管成效进行分析；执行信用主体在各部门的信用状况横向比对，发现问题及时预警；支持各重点领域构建以信用为基础的新型行业监管机制，推送信用主体信用等级给相关政府部门自主参考。

系统功能主要包括：分级分类监管事项清单管理、行业分级分类监管主题数据推送、信用监管留痕管理、信用监管专题分析、信用监管综合分析等。

8、政务诚信管理系统

制定并明确政务信用信息分类和采集目录，实现政务信用信息归集、交换和整合，构建政府部门和公务员政务领域信用主题库，提供政务诚信教育、重点领域政务诚信公示等应用服务功能，实现对失信政府部门和公务员的信用监管。

系统功能主要包括：政务诚信目录管理、政务诚信主题库、政务诚信教育管理、政务领域信用档案管理、重点领域政务诚信监管等。

9、合同履行管理系统

以合同履行信息的归集、共享和应用为主线，对相关合同的签约、履约、违约信息进行标准化处置和分析，对合同履行全流程情况进行跟踪、预警、处置、评价等处理，并通过履约信息在一定范围内的共享应用，促使合同实施主体履约践诺；同时，为政府部门和金融服务机构在企业项目审批、政策扶持、融资授信等方面提供信息支撑。

系统功能主要包括：合同目录清单管理、合同履行归集管理、合同履行自主申报、合同履行信息处理、合同履行信息公示、合同履行信息跟踪分析等。

10、公共信用服务系统

建设信用报告管理系统，按照国家印发的公共信用信息报告标准（2021年版），为各类用户提供高效、规范、权威的信用报告查询服务。

系统功能主要包括：信用修复系统、异议处理系统。

建设信用修复系统，提供方便快捷的信用修复渠道，实现信用修复的发起、收件、审核、办理和反馈全流程管理，实现与“信用中国”网站“双公示”信息信用修复联动处理。为信用主体提供信用修复申请操作平台，当信用主体发现查询报告或网站公示栏目存在不良信用信息时，可向信用主管部门、信用信息提供部门提出书面修复申请或在线修复申请，相关部门登录系统办理信用修复申请，及时反馈办理情况。

建设信用平台异议处理系统，提供信用信息异议的申请发起、收件、审核、办理和反馈全流程管理。为信用主体提供异议申请操作平台，当信用主体对平台内信用信息的真实性、准确性有异议时，可向信用服务部门提出书面核实申请或通过平台提出在线异议申请，相关部门登录系统办理异议申请，及时反馈办理情况。

11、“信易+”应用管理系统

信用信息应用是信用体系建设的重要环节，结合儋州特点、产业优势，在“信易批”、“信易租”、“信用+港口监管”方面开展信用信息应用，对信用信息和信用报告的查询、信用监管和信息推送等方面提供支撑。

根据实际情况探索创新开展“信易+”守信激励工作，扩大“信易+”应用场景，丰富守信激励内容，向符合支持条件的诚信主体提供优质高效的“信易+”服务，让守信者的便利越来越多、越来越可感受，让守信的无形价值变成有形价值，让守信有用、守信有感。

系统功能主要包括：“信易批”、“信易租”、“信用+港口监管”。

“信易批”是结合实施信用承诺制度，对符合条件的守信主体在申报材料不齐全的情况下享受“容缺受理”、“容缺审批”、“告知承诺”等便捷服务，进一步延伸信用承诺制工作，加快办理进度的一种方式。

“信易租”是会同租赁公司、产业园、开发开放试验区等，为守信的创业创新公司提供办公设备、办公空间等便捷租赁服务，助力“大众创业、万众创新”。

在“信用+港口监管”方面，针对港口行业的特点，基于企业信用数据支撑部门精准开展信用监管工作，提供信用查询、信用公示、风险预警、事中事后信用监管等功能。

12、与省发改委省级信用信息平台信息共享对接

全国信用信息共享平台（海南儋州）二期需要与海南自由贸易试验区信用信息共享平台进行数据共享交换，实现信用信息的数据交换互补。截止目前海南自由贸易港信用信息共享平台对接省级部门 74 个，市县级部门 20 个，归集信用数据总量 2.58 亿条，双公示数据归集总量 30.6 万条，红黑名单数据归集总量 2260.99 万条。

系统功能主要包括：信息共享目录管理、信息共享订阅接收、信息共享批量推送等。

三、系统性能要求

1、服务系统支持在线用户数不小于 100；

2、系统不间断运行能力：信用信息平台及相关应用系统需保证 7*24 小时的稳定运行。

3、系统稳定性：系统环境无故障时间达到 99%。

4、数据处理能力

（1）实现信用数据的批量导入速度达到每分钟 10000 条记录的处理能力。

（2）数据解析速度不小于每秒 1000 条，增量检查速度不小于每秒 1000 条，规则检查速度不小于每秒 1000 条，关联比对速度不小于每秒 1000 条，主题数据生成不小于每秒 1000 条。

5、信息访问能力

（1）信用报告审查时涉及法人基本信息、行政处罚信息、红黑名单信息等众多信息类型，在不考虑网络传输时间延迟情况下，单笔核查报告实时查询所需时间在 3 秒之内；若考虑网络传输时间延迟则在 5 秒之内。

（2）批量非实时处理一般建议最低保证第二天返回查询结果，根据业务处理要求批量处理一般应达到每秒 4-5 笔。常用报表及汇总分析响应时间不超过 10 秒。

6、根据系统的安全保密需求，对使用权限划分、身份鉴别、访问控制、安全审计、信息完整性检验等内容进行重点设计与建设。

四、系统安全要求

本项目新增和升级的系统部署在省政务云平台上，通过电子政务外网及互联网进行远程访问。网络安全基础设施建设依托省政务云和电子政务外网的相关安

全设备及安全保障机制。

全国信用信息共享平台（海南儋州）二期项目，搭建在政务云上，按照网络信息安全等保三级要求建设。

五、工具软件采购

1、数据库

根据业务要求，需要采购国产数据库企业版产品 2 套，用于信用平台、信用网站的数据存储。

要求：符合 SQL92 标准，支持 CREATE、ALTER、DROP 等 DDL 语法，支持 SELECT、INSERT、UPDATE、DELETE 等 DML 语法，支持单表，多表联合查询；符合并支持 CAPI、ODBC、JDBC、ADO.NET 等国际接口规范；支持如下的操作系统和平台：64 位 Linux 系列（CentOS、Red Hat、SUSE、Red Flag Asianux）等；支持 BOOLEAN 布尔数据类型大对象数据类型；扩展性强，变更灵活，可以根据实际业务需要灵活部署和配置。

2、中间件

根据业务要求，需要采购国产应用服务器软件产品 5 套，用于 N 应用系统的部署发布管理，满足支撑应用服务器的日常运行管理。

要求：支持 Windows、Unix、Linux 等主流操作系统，实现了 Java EE 规范、最新的 Web 服务标准和主流的互操作标准；它提供高级消息传输、Web 服务、高可用性、集群和多平台支持。

六、项目实施要求

承建单位必须按照国家软件工程标准规范组织系统开发，开发工作可分为需求分析、系统设计、软件编码、系统测试、验收等阶段。

项目承建方须组成开发团队，合理制定开发计划，保证系统开发进度和质量要求，按时完成项目建设内容。

（一）项目组人员要求

在本项目的执行过程中，核心技术人员要按时保质完成本项目，并且整个项目团队的人员要相对稳定。

按照项目实施的要求，必须配置相应的项目管理、系统设计、开发、测试、集成、培训、质量保证等人员，在项目组织中应明确各岗位的职责，确保工程顺

利实施。

参与此项目的核心技术人员必须具有承担过相关软件开发和相关项目建设经验，能够与政府用户进行良好的沟通，掌握信用和电子政务业务的相关基础知识，具有强烈的服务意识和高度的责任感。

对上述安排供应商应列出详细实施计划，包括人员姓名、学历和在本项目中的职责分工。

调整原则。承建方在项目建设期间不得调整项目经理和技术负责人，如确有特殊情况需要变动某些人员，须向项目管理服务方和采购人提出书面申请。

（二）施工进度要求

按软件工程要求，开发工作分为需求分析、系统设计、编码、测试、试运行、项目验收等阶段。承建单位应在保证系统质量的前提下做好项目总体进度控制。

项目建设分三个阶段：

- （1）2022年10月—2022年12月：项目系统开发和实施；
- （2）2023年01月—2023年02月：项目初验，系统试运行；
- （3）2023年06月：项目终验。

（三）交付成果与验收要求

1、交付成果要求

（1）承建方应按照 GB/T 8567—2006《计算机软件文档编制规范》等国家标准要求形成全面的技术资料，包括可运行的程序、源代码及技术文档等，确保技术资料的一致性、完整性和可操作性。

（2）承建方提供的文档和资料均应以磁介质（或光盘）和纸张为载体，文件格式为 Word 文档或其他可视化文件。

（3）提交的设计文档、源程序代码、运行程序三者必须一致。

（4）需提交的文档一览表

序号	工作阶段	各阶段提交成果
1	前期阶段	项目开发计划和方案
2	需求分析	软件需求分析报告
3	系统设计	系统总体设计、系统详细设计、数据库设计说明书
4	系统编码	程序的源代码及说明

5	软件测试	集成测试方案、测试报告、用户操作手册、安装维护手册
6	系统验收	项目总结报告、系统试运行报告
7	培 训	培训计划、培训材料
8	其 它	项目工作周报、月报

2、验收要求

系统整体功能交付达到了全部规定要求，系统上线后稳定运行，通过项目监理方认可，且在提交全部相关文档、报告、源代码等交付物的前提下，由承建方向采购方提出系统竣工验收申请，并组织领域专家进行验收评审，采购人按照验收标准和专家意见进行验收。验收内容和标准包括：

(1) 系统业务功能验收

验收依据包括，《需求规格说明书》、双方签订的合同、建设过程中双方签订的工作备忘记录。

确认系统实现的业务功能完备、正确、满足用户的需求。

(2) 系统性能验收

以供需双方确认的《需求规格说明书》所定义的性能要求为依据。

确认系统的性能满足《需求规格说明书》的要求。

(3) 数据验收

保证数据由原系统移植到新系统的正确无误。

保证系统本身不产生新的错误数据。

(4) 软件过程文档验收标准

文档内容验收标准：文档内容全面、真实、丰富，能清楚阐述实施内容。

文档格式验收标准：文档格式与项目实施要求文档规范相符，文档具有详细的修改记录，版权、作者、时间等信息，包括完整的页眉、页脚等信息。

文档一致性验收：需求文档、设计文档、源程序与目标代码及其他可交付物保持一致。

(5) 系统使用管理制度

满足系统上线运行要求的相关制度和规范。

系统验收前完成项目正式移交，承建方应将完整的各类档案、施工文档、驱

动程序、软件、示例程序源代码、技术文档全部提供给建设方。

（四）保密要求

本项目要求实施方在实施方案中针对本项目建设内容制定保密措施并在项目实施过程中严格执行，以保证项目的成功实施。实施方必须提供对本项目的保密承诺。

（五）培训要求

承建方要根据工程实施的进度及时安排培训和授课。负责对采购人相关部门及指定的用户进行应用性的培训。编制系统用户培训手册。培训的主要内容侧重于对该系统的使用及系统的基本维护、常见问题及解决办法等，并提供实践性的操作，旨在使受培训者熟悉系统设计的思路，掌握系统的操作和维护等。采购人负责对培训质量的监控，并有权对培训内容提出改正意见。

主要的培训包括：

1. 业务人员操作培训

面向应用软件及交换平台的一般工作人员，主要是用户操作培训。由中标单位具有丰富经验的培训师以及产品提供商培训师主讲，对系统和交换平台相关工作人员进行系统的操作培训，配以实际操作的指导，并提供全部详细的培训资料。

2. 系统管理员技术培训

考虑到系统和交换平台的系统管理员的职责除了保证系统正常运转外，还为其他用户提供技术支持，或者在原有基础上进行部分应用功能的扩展。

七、售后服务要求

自终验通过之日起，进入系统免费维护期。在免费维护期内，承建单位需要向采购方提供系统维护服务。在本项目建设中，承建方必须严格履行下述维护义务：

（一）项目平台免费维护期：自终验通过之日起算，提供一年免费质保维护。运维内容主要包括采购设备的维护，改正性维护，即在软件使用过程中识别和纠正软件错误，改正软件性能缺陷；适应性开发服务，即当软件外部环境或数据环境发生变化，修改软件以适应变化。质保期内，所有软件维护升级等均为免费。

（二）在免费维护期内，承建方应始终通过电话服务、远程服务和现场服务向采购方提供快速、高效的维护服务。

(三) 免费维护期间, 承建方应向采购方提供售后服务, 并提供 7*24 小时服务热线, 一般故障排除时间不超过 1 小时, 重大故障排除时间不超过 4 小时。

(四) 每季度一次对最终用户所购系统进行现场维护保养、咨询、升级服务, 及时发现并解决问题, 并提交相应运维检查报告。

(五) 在用户方使用主流品牌的硬件、软件产品出现兼容性问题时, 配合有关硬件、软件厂商和最终用户分析问题原因、协助其寻求解决方案。

(六) 在系统试运行后, 承建方的技术人员到使用现场对整个系统性能进行调优服务, 以确保整个系统的安全、高效运行。

(七) 承建方应配备专门的技术服务部门负责对用户的全方位的技术支持和服务, 提供电话咨询、传真、邮件、现场服务等方式, 以最快的速度响应采购方的请求, 处理用户系统中出现的各种问题和故障, 以保证用户系统的正常运行。

(2) 商务要求

1、**采购标的时间:** 2022 年 9 月

2、**采购标的地点:** 采购人指定地点

3、**交付时间 (期限):**

按软件工程要求, 开发工作分为需求分析、系统设计、编码、测试、试运行、项目验收等阶段。承建单位应在保证系统质量的前提下做好项目总体进度控制。

项目建设分三个阶段:

(1) 2022 年 10 月—2022 年 12 月: 项目系统开发和实施;

(2) 2023 年 01 月—2023 年 02 月: 项目初验, 系统试运行;

(3) 2023 年 06 月: 项目终验。

4、**交付地点 (范围):** 采购人指定地点

5、**付款条件 (进度和方式):** 合同签订支付合同额的 35%, 初验支付合同额的 45%, 验收支付合同额的 15%, 验收之日起满一年支付合同额的 5%。

6、**售后服务:**

自终验通过之日起, 进入系统免费维护期。在免费维护期内, 承建单位需要向采购方提供系统维护服务。在本项目建设中, 承建方必须严格履行下述维护义务:

(一) 项目平台免费维护期: 自终验通过之日起算, 提供一年免费质保维护。

运维内容主要包括采购设备的维护，改正性维护，即在软件使用过程中识别和纠正软件错误，改正软件性能缺陷；适应性开发服务，即当软件外部环境或数据环境发生变化，修改软件以适应变化。质保期内，所有软件维护升级等均为免费。

（二）在免费维护期内，承建方应始终通过电话服务、远程服务和现场服务向采购方提供快速、高效的维护服务。

（三）免费维护期间，承建方应向采购方提供售后服务，并提供 7*24 小时服务热线，一般故障排除时间不超过 1 小时，重大故障排除时间不超过 4 小时。

（四）每季度一次对最终用户所购系统进行现场维护保养、咨询、升级服务，及时发现并解决问题，并提交相应运维检查报告。

（五）在用户方使用主流品牌的硬件、软件产品出现兼容性问题时，配合有关硬件、软件厂商和最终用户分析问题原因、协助其寻求解决方案。

（六）在系统试运行后，承建方的技术人员到使用现场对整个系统性能进行调优服务，以确保整个系统的安全、高效运行。

（七）承建方应配备专门的技术服务部门负责对用户的全方位的技术支持和服务，提供电话咨询、传真、邮件、现场服务等方式，以最快的速度响应采购方的请求，处理用户系统中出现的各种问题和故障，以保证用户系统的正常运行。

7、知识产权归属：

本项目所产生的相关知识产权、产物以及数据均归招标人所有。中标方应保证本项目实施过程中不得侵犯第三方知识产权。

2.B 包： 监理服务

（1）技术要求如下：

一、 监理技术要求

1、 监理服务周期

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。

2、 监理范围

重点对项目建设过程中设备/材料的采购、设备安装调试、系统集成、软件开发及应用技术培训、试运行、测试、验收等全过程进行监督管理，从硬件监理、软件监理、系

系统集成监理等三个方面梳理该项目的工程监理应如何通过切实有效方式、方法、手段达到建设方所要求的深度、广度，最终实现工程监理的目标。实现对质量、进度、经费、变更的控制及合同管理和文档管理。当工程质量或工期出现问题或严重偏离计划时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

3、监理目标控制方案

以工程建设合同、监理委托合同、国家（GB/T19668.1-19668.6《信息化工程监理规范》、工信部信[2002]570号《信息系统工程监理暂行规定》）及有关法规、技术规范与标准、项目建设单位需求为依据，通过专业的控制手段，协助建设单位全面地进行技术咨询和技术监督，对工程全过程进行监督、管理、指导、评价，并采取相应的组织措施、技术措施、经济措施和合同措施，确保建设行为合法、合理、科学、经济，使建设进度、投资、质量达到建设合同规定的目标。

1) 监理质量目标控制

监理质量目标控制是监理技术的核心所在，也是监理单位综合实力的最好反映，所以做好监理质量目标控制方案，确保本项目建设质量能达到建设单位要求的质量目标。

确保本项目建设质量达到工程合同中规定的功能、技术参数等目标。

确保工程建设中的设备和各个节点满足相关国家（GB/T19668.1-19668.6《信息化工程监理规范》、工信部信[2002]570号《信息系统工程监理暂行规定》）地方或行业质量标准和技术标准，按照承建合同要求进行基于总体方案的细化设计、开发、安装、调试和运行；系统集成和软件开发过程涉及用户需求调研分析、概要设计、详细设计、系统实现、系统测试和系统运行等比较复杂、制约因素多的工作内容，应该成为质量控制的重点；深化设计方案的确定、开发平台选定，也要进行充分论证。

要求监理在整个工程实施过程中做好对工程质量的事前控制，事中监督和事后评估，以确保工程质量合格。

投标人应针对本项目建设中软硬件设备采购、设备安装调试、系统集成、软件开发、工程培训等提出工程监理的质量控制原则、方法、措施、工作流程和目标。

2) 监理进度目标控制

确保本项目按合同规定的工期完工。

依据合同所约定的工期目标，在确保质量和安全的原则下，采用动态的控制方法，对进度进行主动控制，确保项目按规定的工期完工。

通过对本项目概要设计的分析、研究，提出针对本项目建设的、有代表性的信息工程监理进度控制的主要原则、方法、内容、措施、工作流程和目标。

3) 监理投资目标控制

协助用户控制本项目建设总投资在项目预算及审计范围内，减少项目建设中的额外开支。

以项目建设方和承建单位实际签订的合同金额为准，确保项目费用控制在合同规定的范围内。

4) 监理项目变更控制

协助用户对本项目的整体进行工期进度、资金、技术等方面进行变更管理、审核。

以项目建设方和承建单位的可研、招投标文件，以及签订的合同建设内容为监理依据，确保项目实施控制在规定的范围内没有遗漏，如有则需进行变更流程。

在项目建设中，合理减少项目变更，保护建设单位的经济利益。

4、工程监理重点难点分析

投标人应根据本项目建设的特点，从实际出发分析本项目监理工作的重点、难点，并根据分析的结果制定相应的监理工作规划、对策和策略，以便日后有针对性的开展建设工程的监理服务工作。

(一) 项目组织及总体技术方案的质量控制

- 1、协助审查项目建设方的投标书、合同及实施方案；
- 2、在技术上、经济上、性能上和风险上进行分析和评估，为采购人提供建议；
- 3、协助审查项目建设方提交的组织实施方案和项目计划等相关文档；
- 4、协助审查项目建设方的工程质量保证计划及质量控制体系；
- 5、参与制定项目质量控制的关键节点及关键路径。

(二) 项目质量控制

1、组织措施：建立质量管理体系，完善职责分工及有关质量监督制度，落实质量控制责任。

2、系统集成质量控制

- 审核系统总集成方案；
- 对采购的硬件设备及网络环境的综合质量进行检验、测试和验收；
- 参与制定系统验收大纲；
- 对设备安装、调试进行验收；
- 对系统进行总体验收。

3、人员培训的质量控制

- 协助审查并确认培训计划，审定培训大纲；
- 监督审查建设方实施其培训计划，并征求采购人的意见反馈；
- 监督审查考核工作，评估培训效果；
- 协助审核并确认培训总结报告。

4、文档、资料的质量控制

监督审查建设方提供的设备型号、数量、到货时间以及设备的技术资料、系统集成和软件安装在实施过程中所有相关文件的标准性和规范化，在各项目验收时，应监督项目建设方提交符合规定的成套资料，包括印刷本和电子版。

对监理项目实施过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版。

（三）进度协调控制

1、组织措施：建立进度控制协调制度，落实进度控制责任。

2、编制项目控制进度计划：编制项目总进度计划和网络图。按各子系统实际情况进行编制，包括系统建设开工、设备的采购、设备的安装调试、软件的编制、试运行等各方面内容,做到既要保证各子系统、各阶段目标的顺利实现，又要保证项目间、阶段间的衔接、统一和协调。

3、审查各子系统建设方编制的工作进度计划：分析系统建设进度计划是否能满足合同工期及系统建设总进度计划的要求，特别要对照上阶段计划工程量完成

情况进行审查，对为完成系统建设进度计划所采取的措施是否恰当、设备能否满足要求、管理上是否有缺陷进行审查。要根据建设方所能提供的人员及设备性能复核、计算设备能力和人员安排是否满足要求等，分析判断计划是否能落实，审查建设方提出的设备供应计划能否落实。如发现供应计划未落实，应及时报告采购人，要求建设方采取应急措施满足系统建设的需求。

4、系统建设进度的现场检查：随时或定期、全面地对进度计划的执行情况跟踪检查，发现问题及时采取有效措施加以解决。加强系统建设准备工作的检查，在工程项目或部分工序实施前，对情况进行检查，要加强检查设备、人员安排、各项措施的落实情况，确保准备工作符合要求，不影响后续工程的进行。

5、进度计划的分析与调整：要保证建设进度与计划进度一致，经常对计划进度与实际进度进行比较分析，发现实际进度与计划进度不符时，即出现进度偏差时，首先分析原因，分析偏差对后续工作的影响程度，并及时通知建设方采取措施，向建设方提出要求和修改计划的指令。

（四）投资控制

- 1、组织措施：建立健全项目管理组织，完善职责分工及有关质量项目管理制度，落实投资控制的责任。
- 2、审查设计图纸和文件，审查建设方的施工组织设计和各项技术措施，深入了解设计意图，在保证系统建设质量和安全的前提下尽可能优化设计。
- 3、严格督促建设方按合同实施，严格控制合同外项目的增加，协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度；及时了解系统建设情况，协调好各方矛盾，减少索赔事件的发生。对发生的事件严格按合同及法律条款进行处理，认真进行索赔调解。

（五）合同管理

合同管理是加快系统建设进度、降低系统建设造价、保证系统建设质量的有效途径之一。通过合同管理，可以督促建设方在各个阶段按照合同要求保证设备、人员的配备及投入，保证各阶段目标按合同实施，减少索赔事件，控制系统建设结算等。具体要求如下：

1、以合同为依据，本着“实事求是、公正”的原则，合情合理地处理合同执行过程中的各种争议。

2、分析、跟踪和检查合同执行情况，确保项目建设方按时履约。

3、对合同的工期的延误和延期进行审核确认。

4、对合同变更、索赔等事宜进行审核确认。

5、根据合同约定，审核项目建设方的支付申请。

6、建立合同目录、编码和档案。

7、合同管理坚持标准化、程序化，如设计变更、延期、索赔、计量支付等应规定出固定格式和报表。合同价款的增减要有依据，合同外项目增加要严格审批制度。重大合同管理问题的处理，如大的变更、索赔、复杂的技术问题等，组成专门小组进行研究。不符合实际情况的合同条款及时向采购人报告，尽早处理，以免造成损失。

（六）信息、工程文档管理

在项目管理过程中，为了实现对进度、质量、投资的有效控制，处理有关合同管理中的各种问题，监理方需要收集各种有用的信息。信息的来源主要包括采购人文件、设计图纸和文件、建设方的文件、建设现场的现场记录（或项目管理日志）会议记录、验收情况及备忘录等等。其中项目管理日志是进行信息管理的一个最重要的方面。项目管理日志主要包括当天的工作项目和工作内容、投入的人力和设备运行情况、计划的完成情况、进度情况、停工和返工及窝工情况。信息管理主要措施要求如下：

1、制定详细的信息收集、整理、汇总、分析、传递和利用制度，力求信息管理的标准化和制度化。由专人负责系统建设信息的收集、分类、整理储存及传递工作。信息传递以文字为主，统一编号，利用计算机进行管理，力求信息管理的高效、迅速、及时和准确，为系统建设提供及时有用的信息和决策依据。

2、在项目实施过程中做好工程监理日记和工程大事记。

3、做好双方合同、技术建设方案、测试文档、验收报告等各类往来文件的存档。

4、建立必要的会议、例会制度，整理好会议纪要，并监督会议有关事项的执行情况。

5、立足于建设现场，加强动态信息管理，对现场的信息进行详细记录和分析，做到以文字为基础，以数据说明问题。根据收集到的信息与合同进行比较，督促建设方的人员和设备到位，促使承包商按合同完成各项目标，从而实现对进度、质量、投资的控制。

6、建立完整的各项报表制度，规范各种适合本项目的报表。定期将各种报表、信息分类汇总，及时向采购人及有关各方报送。

7、监理项目验收时，应提交符合规定的有关工程的成套资料，包括印刷本和电子版。

（七）日常监理

1. 掌握监理范围内涉及的各种技术及相关标准；

2. 安排足够的监理人员，成立项目监理部，按工程需要派驻相应的专业人员进行项目现场监理，随时为采购人提供服务，总监理工程师必需专职于本项目；

3. 制定工程管理的组织机构方案并协助采购人组建相关机构，并提供相关培训；

4. 熟悉了解项目的业务需求，协助采购人对项目的目标、范围和功能进行界定，参与并协助项目的设计方案交底的审核工作；

5. 建立健全科学合理的会议制度，并予以贯彻落实；

6. 建立健全科学合理的文档管理制度，制订开发过程中产生的各类文档制作、管理规范，并予以贯彻落实；

7. 与采购方一起制定评审机制，在工程实施全过程中随时关注隐患苗头，如发现将会导致工程失败的情况出现时，应及时启动评审机制，组织专家对工程实施情况进行评审，对评审不合格的，应向采购方提出终止合同意见。此外，还应组织定期评审（阶段性评审、里程碑评审、验收评审）对评审结果为优的，提出奖励意见，评审不合格的，则向采购方提出处理意见。

5、工程各阶段的监理规划、实施

投标人应对本项目从设计施工到项目竣工验收阶段制定一整套工程监理的工作

流程，并叙述各阶段主要监理工作内容。

本项目监理工作主要分为设备/材料采购、施工阶段、验收阶段、质保期阶段等。

(1)、设备/材料采购监理

建设项目由承包单位承担设备/材料采购任务，工程监理单位在设备/材料采购阶段监理工作主要有：

- ◇ 审核承包单位的设备采购计划和设备采购清单；
- ◇ 订货进货验证；
- ◇ 组织到货验收；
- ◇ 鉴定、设备移交等；

(2)、施工阶段监理

1、开工前的监理

1) 审核施工设计方案：开工前，由监理单位组织实施方案的审核，内容包括设计交底，了解需求、质量要求，依据设计招标文件，审核总体设计方案和有关的技术合同附件，以避免因设计失误造成实施的障碍；

2) 审核实施方案的合法性、合理性、与设计方案的符合性；

3) 审批施工组织设计：对施工单位的实施工作准备情况进行和监督；

4) 审核施工进度计划：对施工单位的施工进度计划进行评估和审查；

5) 审核实施人员：确认施工方提交的实施人员与实际工作人员的一致性，如有变更，则要求叙述其原因；

6) 审核《软件项目开发计划》。

2、施工准备阶段的监理

1) 审批开工申请，确定开工日期；

2) 了解承包商设备订单的订购和运输情况；

3) 了解施工条件准备情况；

4) 了解承建单位实施前期的人员组织、施工设备到位情况；

5) 编制各个子项目监理细则；

6) 签发开工令。

3、施工阶段的监理

- 1) 审核软件开发各个阶段文件;
- 2) 协助采购人组织软件开发阶段评审;
- 3) 材料、硬件设备、系统软件的供货计划的审核;
- 4) 材料、硬件设备、系统软件的进场、开箱和检验;
- 5) 促使项目中所使用的产品和服务符合合同及国家相关法律法规和标准;
- 6) 对施工各个阶段的安装工艺进行检查;
- 7) 审核项目各个阶段进度计划;
- 8) 督促、检查承建单位进度执行情况;
- 9) 审查项目变更, 提出监理意见;
- 10) 审查承建单位阶段款支付申请, 提出监理意见;
- 11) 按周(月、旬)定期报告项目情况;
- 12) 组织召开项目例会和专项会议。

4、试运行阶段的监理

- 1) 协助建设方确认项目进入试运行;
- 2) 监查系统的调试和试运行情况, 记录系统试运行数据;
- 3) 进行试运行期系统测试, 做出测试报告;
- 4) 对试运行期间系统出现的质量问题进行记录, 并责成有关单位解决。解决问题后, 进行二次监测;
- 5) 进行试运行时间核算;
- 6) 协助业主确认试运行通过。

(3)、验收阶段监理

1、验收阶段

- 1) 依照国家信息化管理细则, 国家验收管理办法约定执行。
- 2) 对承建单位在试运行阶段出现的问题的整改情况进行监督和复查;
- 3) 监督检查承建单位作好用户培训工作, 检查用户文档;
- 4) 组织系统初步验收;
- 5) 审查承建单位提交的竣工文档;
- 6) 参与项目竣工验收;
- 7) 竣工资料收集整理齐全并装订, 签署验收报告;

- 8) 审核项目结算;
- 9) 审查承建单位阶段款支付申请, 提出监理意见;
- 10) 向建设单位提交监理工作总结;
- 11) 将所有的监理材料汇总, 编制监理业务手册, 提交采购人;
- 12) 系统验收完毕进入保修阶段的审核与签发移交证书。

2、项目移交阶段

- 1) 系统的设计方案、设计图纸和竣工资料的全部移交;
- 2) 设备、软件、材料等的验收文档核实;
- 3) 施工文档的移交;
- 4) 竣工文档的移交;
- 5) 项目的整体移交。

(4)、质保期阶段监理

监理单位承诺依据委托监理合同约定的工程质量保修期规定的时间、范围和内容开展工作主要有:

- 1) 定期对项目进行回访, 协助解决技术问题;
- 2) 对项目建设单位提出的质量缺陷进行检查和记录;
- 3) 对质量缺陷原因进行调查分析并确定责任归属;
- 4) 检查承建单位质保期履约情况, 督促执行;
- 5) 审查承建单位阶段款支付申请, 提出监理意见。

投标人应根据上述监理工作内容(但不局限于上述内容)分别制定详细的监理工作流程, 使本项目的监理工作流程化、制度化。

3.1 监理工作要求

1、监理工作制度要求

根据本项目的特色, 本项目要求以现场监理为主要方式进行, 在施工现场主要监理人员必须具备所从事监理业务的专业技术和类似系统经验, 并具有丰富的项目管理经验。本次监理项目实行总监理工程师负责制, 在整个项目建设期间, 总监理工程师必须保证有三分之一工作日以上的时间到甲方现场, 且必须在建设期间全程常驻至少一名监理工程师在甲方现场进行监理协调调度。监理公司应建立项目监理小组, 负责整个项目

的全程监理工作。监理人员的确定和变更，须事先经业主方同意。监理人员必须奉公守法，具有高度的责任心。

2、监理项目组织要求

工程监理组织形式应根据工程项目的特点、工程项目承包模式、业主委托的任务以及监理单位自身情况而确定，结构形式的选择应考虑有利于项目合同管理、有利于目标控制、有利于决策指挥、有利于信息沟通。

要求投标人在报价方案中要明确工程监理的各项运作，包括监理人员的相关资料、职能分配、监理组织的构成及工作流程、各项监理工作的相关负责人等。

3、监理信息管理要求

投标人应制定有关本项目信息管理流程，规范各方文档并负责整理记录归档业主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，并定期以监理月（周/季）报形式提交业主。包括下列监理工作：

- 1) 做好监理日记及工程大事记；
- 2) 做好合同批复等各类往来文件的批复和存档；
- 3) 做好项目协调会、技术专题会等各项会议纪要；
- 4) 管理好实施期间的各类、各方技术文档；
- 5) 做好项目周报；
- 6) 做好监理建议书、监理通知书存档；
- 7) 阶段性项目总结。

投标人应针对项目特点，制定相应的信息分类表、信息流程图、信息管理表格、信息管理工作流程与措施，同时要求采用先进的项目信息管理软件对项目信息进行综合管理。

4、监理合同管理要求

本项目建设过程中会与承建单位签订各种合同，投标人应该针对项目特点制定合同从草案到签署的管理工作流程与措施，规范合同管理，并在具体项目合同执行时进行下列监理工作：

- 1) 跟踪检查合同的执行情况，确保承建单位按时履约；

- 2) 对合同工期的延误和延期进行审核确认;
- 3) 对合同变更、索赔等事宜进行审核确认;
- 4) 对合同终止进行审核确认;
- 5) 根据合同约定, 审核承建单位提交的支付申请, 签发付款凭证;
- 6) 要求对项目合同进行合理的管理, 以完善整个项目建设的过程。

二、监理服务准则

遵照国家GB/T19668.1-19668.6《信息化工程监理规范》、工信部信[2002]570号《信息系统工程监理暂行规定》的规定, 以“守法、诚信、公正、科学”的准则执业, 维护建设方与承建方的合法权益。具体应做到:

- 1) 执行有关项目建设的法律、法规、规范、标准, 履行监理合同规定的义务和职责。
- 2) 不收受被监理单位的任何礼金。
- 3) 不泄漏所监理项目各方认为需要保密的事项。
- 4) 遵守国家的法律和政府的有关条例、规定和办法等。
- 5) 坚持公正的立场, 独立、公正地处理有关各方的争议。
- 6) 坚持科学的态度和实事求是的原则。
- 7) 在坚持按监理合同的规定向建设单位提供技术服务的同时, 帮助被监理者完成起担负的建设任务。
- 8) 不泄漏所监理的项目需保密的事项。

三、监理依据

- 1) 国家GB/T19668.1-19668.6《信息化工程监理规范》、工信部信[2002]570号《信息系统工程监理暂行规定》和国家有关信息系统项目建设和监理管理规范;
- 2) 建设单位与承建单位签订的承包工程合同
- 3) 建设单位与监理单位签订的委托监理合同
- 4) 本工程招标书、招标过程文件、各中标商的投标书
- 5) 国家有关合同、招投标、政府采购的法律法规
- 6) 部颁、地方政府的信息工程、信息工程监理的管理办法和规定
- 7) 建设工程和信息工程相关的国家、行业标准和规范

- 8) 建设工程和信息工程技术监督、工程验收规范
- 9) 与工程相关的技术资料
- 10) 其他与本项目适用的法律、法规和标准
- 11) 国家、地方及行业相关的技术标准

四、安全保密要求

本项目要求投标人制定一整套工程监理安全保密制度，确定工程保密责任人，同时要求投标人：

- 1) 按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议；
- 2) 监理单位各级组织严格履行保密职责；
- 3) 按照公司内部保密规定开展监理工作。

五、监理验收要求

1) 审核监理方应提交的各类监理文档和最终监理总结报告，综合评估监理方在系统开发进度、质量把关、重难点问题解决、项目投资等方面的监理情况。只有文档齐全，系统开发工作中没有出现重大质量事故才予验收。

- 2) 本监理工作的最终验收由主管部门组织，项目通过验收即为验收通过。

六、其它要求

1. 监理总工程师

- 1) 具有国家主管部门颁发的信息系统监理师资格；
- 2) 5年以上监理或项目管理经验。

2. 监理工程师

- 1) 具有国家主管部门颁发的信息系统监理师资格；
- 2) 2年监理或项目管理经验。

3. 项目管理及施工组织

投标人须提供详尽的监理技术方案，包括但不限于施工组织部署、项目管理目标、施工准备、进度控制、质量管理、验收方法等内容。

(2) 商务要求

- 1、**采购标的时间：**2022年9月
- 2、**采购标的地点：**采购人指定地点
- 3、**服务工期：**签订合同之日起，至建设项目完成竣工验收
- 4、**交付地点（范围）：**采购人指定地点
- 5、**付款条件（进度和方式）：**合同约定。
- 6、**监理内容为全国信用信息共享平台（海南儋州）二期项目的全部建设内容。**

3. C包：软件测评

（1）技术要求如下

1. 项目概述

依据“GB/T25000.51-2016 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”相关内容，对本建设项目中的所有软件系统开展第三方软件测试，出具相应的测试报告。

软件测试包括：功能性测试、性能测试、安全性测试。

2. 服务目标

为保障本项目应用系统平台如期上线，需要对项目应用系统进行系统功能性、性能、安全性等测试，通过第三方软件测试服务项目的实施，应用专业的测评方法、手段和工具，充分发现并及时修复系统缺陷，保障相关应用系统的各个需求都被正确开发实施，功能、性能等各项指标满足设计要求，为系统的稳定运行和充分发挥建设成效奠定坚实基础。通过采购专业第三方测试服务，达成如下总体测试目标：

- 1、判定各项目的建设方案、招标方案、需求规格说明书等是否实现；
- 2、判定各项目的建设是否满足国家、海南省各项政策法规及标准要求；
- 3、验证应用系统建设内容是否达到对应的建设目标，形成最终的测试总结报告，作为该项目验收的依据。

3. 测试原则

为确保本项目组织与实施的严谨性、严密性和严肃性，投标人应遵循如下原则执行：

(1) 公平公正原则，投标人应遵循“面向应用、保证质量、客观公正、诚信守诺”的原则，一切以事实为依据，用客观测试数据说话，减少人为主观评判；

(2) 全面性原则：投标人应确保测试的范围覆盖业务需求的所有功能点，包括但不限于正常业务流程验证、异常业务流程验证、各功能合法性验证以及功能逻辑的验证等；

(3) 规范化原则：投标人在进行测试过程中应该采用专业的测试方法，制定合理的测试计划，规范的测试过程管理，确保测试结果正确性、有效性、可预期和可重现，符合本项目验收的所有要求；

(4) 标准化原则：投标人的测试活动应依据现行的国家和行业标准、规范和规定开展，相关国家标准和行业标准如有更新，应以最新的国家标准和行业标准为准。本项目测试所使用的标准和规范与投标方所执行的标准不一致时，应采用较高标准执行。

(5) 回避原则：投标人承诺不从事与本项目产品和服务相关的销售、开发、集成及咨询活动；对本项目的承建方在业务上以及核心技术上不构成竞争关系。

(6) 保密原则：投标人承诺对在测试过程中所涉及的有关本项目财务以及技术方案等方面的资料严格保密。

(7) 优质服务原则：投标人应保证提供符合本测试要求和有关标准的优质服务，并确保测试报告符合项目验收的所有要求。

4. 测试依据

投标人必须依据国家和行业标准、规范进行相关内容的测试，包括但不限于：

- 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》；
- 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》；
- GB/T 25000.23-2019《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第23部分：系统与软件产品质量测量》；

- GB/T 25000.2-2018《系统与软件工程 系统与软件质量要求和评价（SQuaRE）第2部分：计划与管理》；

GB/T 25000.1-2010《软件质量要求与评价（SQuaRE）指南》；

相关国家标准和行业标准如有更新，应以最新的国家标准和行业标准为准。

此外，在测试时，还将依据以下资料：

- 招标人提供的各个项目招标需求文档；
- 软件开发合同及合同实施过程文档；
- 招标人和系统承建方提供的其他相应资料。

5. 测试内容

测试内容应包含全国信用信息共享平台（海南儋州）二期项目的软件部分建设内容。测试内容要求如下表所示：

检测内容		备注
全国信用信息共享平台（海南儋州）二期项目	功能测试	主要参照软件质量模型，从软件的功能方面进行测评，系统的程序和数据应满足符合功能需求，系统功能应以正确的方式执行。
	性能测试	系统的性能应满足系统的负载要求和性能需求，性能需求可包括：可承受的并发量、响应时间、吞吐量。
	安全性测试	利用各种主流的攻击技术对系统的应用层进行安全检查，主要针对以下常见漏洞进行检测： <ol style="list-style-type: none"> 1. SQL注入漏洞检测 2. XSS跨站脚本漏洞检测 3. 文件上传后面漏洞检测 4. 弱口令漏洞检测 5. 目录遍历漏洞检测 6. 中间件漏洞检测 7. 传输加密检测 8. 授权绕过漏洞检测

检测内容		备注
	9. 权限提升漏洞检测 10. Cookie 安全漏洞检测 11. 跨站请求漏洞检测 安全性测试实施过程需使用获得中国国家信息安全产品认证证书和国家信息安全漏洞库兼容性资质证书的专业漏洞扫描工具，根据漏洞检测结果，进行漏洞分析，说明漏洞的危害程度，并提出整改意见，在用户整改后进行复测，验证是否完成整改，是否通过测试。	

6. 测试质量要求

- (1) 测试报告内容及数据要求准确、完整、客观、公正；
- (2) 测试服务质量应符合评测规范中的相关要求；
- (3) 客观评估建设项目是否达到系统建设的要求，同时技术评测结果或测试报告必须提交最终用户确认。

7. 测试服务要求

(1) 功能性测试

功能性测试的目的是测试验证系统功能实现的完整性、正确性、适合性等是否能满足项目建设需求，以确保需求功能的实现。根据需求规格说明，利用等价类划分法、边界值分析法、错误推测法、因果图法、组合分析法等，编制测试用例、用例流，以核实业务流程及功能实现在使用有效数据时得到预期的结果，在使用无效数据时显示相应的错误消息或警告消息，各业务规则都得到了正确的应用。主要要求如下：

分析被测对象功能需求，依据项目的《需求规格说明书》和《用户使用手册》要求验证系统实现了全部需求，并确保各项功能是可执行的。

根据系统《需求规格说明书》、《安装部署手册》和《用户使用手册》，分析各功能点测试的优先级别。用户经常使用、关系到系统核心功能、优先级别较高的功能点应予以重点关注，尤其在回归测试时应优先执行。

分析应用系统数据处理需求，对系统业务数据进行严格的正确性测试（包括数据是否超出正常的值范围、报表数据准确性等），确保系统实时数据和历史数据准确无误。

测试用例应当覆盖流程的各个分支，确保流程整体符合业务要求。

(2) 性能效率测试

测试系统的性能是否符合预期的要求，从而保证被测系统快速稳定的运行。通过模拟巨大的工作负荷以查看应用程序在峰值使用情况下如何执行操作，确保在系统交付时能够流畅运行。

(3) 安全性测试

安全性测试是通过渗透测试方法测试验证系统是否存在安全隐患，由具备高技能和高素质的安全服务人员发起、并模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，以期发现和挖掘系统中存在的漏洞。

1. 保密要求

(1) 现场保密管理

工作服务现场除应满足被测设备工作环境外，应满足以下要求：

- a) 网络采取和设定密级相适应的防病毒和安全防护等信息安全措施。
- b) 按照设定保密等级要求对现场人员和设备，尤其是可移动存储介质进行管理。
- c) 对本次项目有关的技术文件、数据等，按照设定密级进行管理。

(2) 资料的保密管理和控制

技术资料在项目过程中由项目经理专人保管，项目服务过程所需的技术资料由资料管理员负责收发。任何人不得将技术资料及相关信息透露给第三方。

(2) 商务要求

- 1、采购标的时间：**2022年9月
- 2、采购标的地点：**采购人指定地点
- 3、服务工期：**

(1) 项目实施要求收到开工令之日起20个工作日内提供项目测试方案；测试工作完成并报告确认无误后20个工作日内，提交系统测试报告。

(2) 项目验收要求测试方应提交最终测试总结报告，并按合同要求完成测试工作才予验收。

4、交付地点（范围）：采购人指定地点

5、付款条件（进度和方式）：合同约定。

6、售后服务：

一、网络安全等级保护咨询服务

乙方向甲方提供网络安全等级保护相关的政策、法律法规及技术要求和标准的咨询服务工作。

1.1 咨询服务时间

自合同生效之日起，提供一年免费的网络安全等级保护咨询服务。

1.2 咨询服务方式

在咨询服务时间内，乙方将向甲方提供以下方式进行咨询服务方式。

服务方式具体如下：

序号	服务方式	服务响应
1	电话咨询服务	7*24 小时
2	QQ/微信在线咨询	5*8 小时
3	Email 咨询服务	5*8 小时
4	现场咨询服务	按需

1.3 咨询服务内容

1.3.1 等级保护政策/标准咨询

网络安全咨询服务，作为乙方等级测评售后服务项目之一。

随着国家网络安全等级保护的推进工作，网络安全等级保护政策、法律法规和标准体系也会相应的发布和更新，乙方针对本项目设立网络安全等级保护咨询平台，提供于甲方各部门相关人员咨询，咨询内容包括但不限于网络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。

1.3.2 等级保护对象等级变更咨询

在等级保护对象出现等级变更时，乙方将协助甲方对等级保护对象进行分析，明确等级保护对象边界和定级对象，对等级保护对象的子系统进行划分，确定等

级保护对象以及子系统的安全等级。

1.3.3 等级保护建设整改咨询

按照等级保护对象安全总体方案要求，乙方将结合等级保护对象安全建设项目计划，根据网络安全等级保护相关标准和规定，对甲方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，结合甲方的实际情况，协助甲方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.D 包：网络安全等级保护测评

(1) 技术要求如下

一、项目服务范围

采购人将委托具有网络安全等级测评与检测评估机构服务认证证书的投标人，依据国家网络安全等级保护 2.0 的相关标准和规定，按照《信息安全技术 网络安全等级保护基本要求》(GBT22239-2019)等有关管理规范和技术标准，对采购单位的等级保护对象的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心的技术要求，以及安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理的管理要求，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，出具符合公安机关要求的《网络安全等级保护等级测评报告》，针对等级保护对象安全建设提出具有针对性的整改建议。

1、服务对象

序号	测评系统名称	依据级别
1	全国信用信息共享平台（海南儋州）	第三级(S3A3G3)

二、项目依据

2.1 项目政策法规

- 1) 《中华人民共和国网络安全法》国家主席第五十三号令；
- 2) 《中华人民共和国计算机信息系统安全保护条例》国务院 147 号令；
- 3) 《关于进一步加强信息安全等级保护工作的通知》（琼等保办【2013】2 号）须加快等级测评和安全建设整改；
- 4) 《关于印发儋州市深化信息安全等级保护工作方案的通知》（儋府办【2015】

51 号);

5) 《海南省信息化条例》第三十七条:“使用财政性资金建设以及关系国计民生、社会稳定的信息网络和信息系统投入使用前,应当按照国家和本省有关规定进行信息安全测评。”

2.2 标准

1. 《信息安全技术 网络安全等级保护实施指南》GB/T 25058 - 2019;
2. 《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019;
3. 《信息安全技术网络安全等级保护测评要求》GB/T 28448-2019;
4. 《信息安全技术网络安全等级保护测评过程指南》GB/T 28449-2018;
5. 《信息安全技术网络安全等级保护安全设计技术要求》GB/T 25070-2019;
6. 《信息安全技术网络安全等级保护定级指南》GA/T 1389-2017;
7. 《信息安全技术 信息安全风险评估规范》GB/T 20984-2007。

三、项目服务内容

3.1 网络安全等级保护测评服务

投标人应依据国家网络安全等级保护管理规定,按照《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)、《信息安全技术网络安全等级保护测评过程指南》(GB/T28449-2018)有关管理规范和技术标准对等级保护对象进行确认、分析和梳理,提出详细的等级测评方案,对等级保护对象的整体保护状况和等级保护对象组件,逐一进行网络安全等级保护测评。等级测评的内容包括以下内容: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的安全测评;完成测评工作后,出具《网络安全等级保护等级测评报告》,并针对等级保护对象安全建设提出具有针对性的整改建议。

测评服务对象

序号	测评系统名称	依据级别
1	全国信用信息共享平台(海南儋州)	第三级(S3A3G3)

测评服务范围

序号	测评安全类	依据级别	测评范围
1	安全物理环境	第三级 (S3A3G3)	招标人机房
2	安全通信网络	第三级 (S3A3G3)	核心交换机、汇聚交换机和接入路由器等网络互连设备、防火墙、入侵防范系统等 服务器、虚拟机、操作系统、数据库应用系统各子系统 存储、阵列和备份等
3	安全区域边界	第三级 (S3A3G3)	
4	安全计算环境	第三级 (S3A3G3)	
5	安全管理中心	第三级 (S3A3G3)	
6	安全管理制度	第三级 (S3A3G3)	管理机构设置、管理制度、操作规程及相关记录表单
7	安全管理机构	第三级 (S3A3G3)	
8	安全管理人员	第三级 (S3A3G3)	
9	安全建设管理	第三级 (S3A3G3)	系统建设相关文档（设计、采购和使用、软件开发、工程实施、验收、交付、测评等）
10	安全运维管理	第三级 (S3A3G3)	环境管理、资产管理、介质管理、设备管理等运维管理

3.1.1 测评实施内容

投标人在测评过程中，按照《信息安全技术 网络安全等级保护测评过程指南》等标准开展测评实施工作，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、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。

3.1.2 测评实施过程

3.1.2.1 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

测评准备工作应包括工作启动、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. 确定测评委托单位应提供的资料	
信息收集 分析	1. 整理调查表单	《等级保护对象调查表》
	2. 发放调查表单给测评委托单位	
	3. 协助测评委托单位填写调查表	
	4. 收回调查结果	
	5. 分析调查结论	
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》打印 各类表单:风险告知书、 文档交接单、会议记录表 单、会议签到表单
	2. 模拟被测定级对象架构,熟悉被测定级对象	
	3. 准备和打印各类表单	

3.1.2.2 方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。

方案编制活动应包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、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	分析并确定被测定级对象 识别并描述被测定级对象的整体结构 识别并描述被测定级对象的边界 识别并描述被测定级对象的网络区域 识别并描述被测定级对象的主要设备 确定测评对象 描述测评对象	《测评方案》的 测评对象部分

二、测评指标确定	确定被测定级对象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
	根据被测定级对象的 A 类、S 类及 G 类基本安全要求的组合情况, 从 GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标	
	根据测评委托单位及被测定级对象业务自身需求, 确定特殊测评指标。	
	对确定基本测评指标和特殊测评指标进行描述, 并分析给出指标不适用的原因	
三、测评内容确定	确定每个测评对象对应的每个测评指标的测评方法	《测评方案》的单项测评实施部分
	确定实施测评的单项测评内容	
四、工具测试方法确定	<p>确定工具测试环境</p> <p>确定工具测试工具</p> <p>确定工具测试的测评对象</p> <p>选择测试路径</p> <p>确定测试工具的接入点</p> <p>本次项目测评需要使用到如下工具:</p> <p>漏洞扫描工具;</p> <p>Windows 主机安全配置检查工具;</p> <p>Linux 主机配置检查工具;</p> <p>网络及安全设备配置检查工具;</p> <p>病毒检查工具;</p> <p>木马检查工具;</p> <p>网站恶意代码检查工具;</p> <p>在线检查工具(网站安全检查工具);</p> <p>终端安全检查工具;</p> <p>口令破解工具;</p>	《测评方案》的工具测试方法及内容部分

	渗透测试工具； SQL 注入验证检查工具； 在线数据库安全检查工具。	
五、测评指导书开发	确定单个测评对象，内容包含测评对象的名称、位置信息、用途、管理人员等信息	测评指导书、测评结果记录表格
	确定单项测评实施活动,包括测评项、测评方法、操作步骤和预期结果等四部分	
	确定单项测评、整体测评表述形式	
	根据测评指导书,形成测评结果记录表格	
六、测评方案编制	明确项目整体情况和测评活动依据	向用户提交经过评审和确认的《测评方案》、《风险规避实施方案》
	根据测评协议书和被测定级对象情况,估算现场测评工作量	
	根据测评项目组成员安排,编制工作安排情况	
	根据以往测评经验以及被测定级对象规模,编制具体测评计划,包括现场工作人员的分工和时间安排	
	汇总上述内容及方案编制活动的其他任务获取的内容形成测评方案文稿	
	评审和提交测评方案	
	根据测评方案制定风险规避实施方案	

3.1.2.3 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,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作主要取得报告编制活动所需的、足够的证据和资料。

现场测评活动应包括现场测评准备、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	测评委托单位对风险告知书签字确认	会议记录，风险告知书，测评方案和现场测评工作计划，现场测评授权书
	测评委托单位协助测评机构签署现场测评授权书	
	召开现场测评首次会	
	双方确认测评计划和测评方案	
	双方确认配合人员、测评环境等各种现场测评需要的资源	
2. 现场测评和结果记录	确认测评对象的关键数据已经进行了备份	《各类测评结果记录/测评证据和证据源记录/文档交接/规划记录单》 访谈结果: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、安全运维管理安全测评的测评结果记录或录音；
	确认具备测评工作开展的条件，测评对象工作正常，系统处于一个相对良好的状况	
	根据测评指导书实施现场测评，获取相关证据和信息	
	测评结束后，双方确认测评工作是否对测评对象造成不良影响, 测评对象及系统是否工作正常	
3. 结果确认和资料归还	汇总测评记录，对漏掉和需要进一步验证的内容实施补充测评	文档审查结果: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

	<p>召开现场测评结束会，测评双方对测评过程中得到的证据源记录进行确认</p>	<p>设管理、安全运维管理测评的测评结果记录；</p> <p>配置核查结果：安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格</p>
	<p>测评人员归还借阅的所有文档资料，并由测评委托单位文档资料提供者签字确认</p>	<p>工具测试结果：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</p> <p>实地察看结果：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、安全运维管理测评结果记录</p> <p>测评结果确认：现场核查中发现的问题汇总、测评证据和证据源记录、测评委托单位的书面认可文件</p>

3.1.2.4 报告编制活动

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项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。报告编制活动应包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成及测评报告编制七项主要任务。

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情况	测评报告的等级测评结果记录部分
	分析单项测评项的测评证据,并与要求内容的预期测评结果相比较,给出单项测评结果和符合程度得分	
	综合判定单项测评项的测评结果	
2. 单元测评结果判定	汇总不同测评对象对应测评指标的单项测评结果情况	测评报告的单元测评小结部分
	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(包括安全控制点、安全控制点间、区域间)之间的关联关系及对结果的影响情况	测评报告的整体测评部分
	根据整体测评分析情况,修正单项测评结果符合程度得分和问题严重程度值	
4. 系统安全保障评估	根据整体测评结果,计算修正后的每个测评对象的单项测评结果和符合程度得分	测评报告的系统安全保障评估部分

	<p>根据各对象的单项符合程度得分, 计算安全控制点得分</p> <p>根据安全控制点得分, 计算安全层面得分</p> <p>根据安全控制点得分和安全层面得分, 总体评价被测定级对象已采取的有效保护措施和存在的主要安全问题情况</p>	
5. 安全问题 风险分析	<p>针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题, 结合关联测评对象和威胁, 分析可能对定级对象、单位、社会及国家造成的安全危害</p> <p>结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危害(损失)结果</p> <p>根据最大安全危害严重程度进一步确定定级对象面临的风险等级, 结果为“高”“中”或“低”</p>	测评报告的安全问题 风险分析部分
6. 等级测评 结论形成	<p>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</p> <p>计算定级对象综合得分, 形成等级测评结论</p>	等级测评报告的等级 测评结论部分
7. 测评报告 编制	<p>概述测评项目情况, 整理前面几项任务的输出/产品</p> <p>针对被测定级对象存在的安全隐患, 提出处置建议</p>	经过评审和确认的被 测定级对象等级测评 报告

	根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息,对测评报告进行评审	
	评审通过后,由项目负责人签字确认并提交给测评委托单位	

3.1.2.5 测评实施活动文档

测评机构在上述各阶段活动的测评实施服务过程中,根据服务规范和采购人要求,提供系统、完整、清晰的服务日常报告。

提供的服务文档应至少但不限于如下文档:

测评准备活动阶段:

- 《项目计划书》;
- 《等级保护对象调查表》;
- 《会议记录表》;

方案编制活动阶段:

- 《网络安全等级保护测评方案》;
- 《测评指导书》;
- 《风险规避实施方案》;

现场测评活动阶段:

- 《现场测评授权书》;
- 《文档交接单》;
- 《会议记录》;

报告编制活动阶段:

按系统提交《网络安全等级保护等级测评报告》,并针对该信息系统提出安全整改建议。

3.2 信息安全等级保护安全建设整改方案设计

在完成安全等级保护测评后,投标人根据本项目相关信息系统的测评报告,针对等级测评过程发现的问题,将依据网络安全等级保护政策法规和标准规范,以及《关于开展信息安全等级保护安全建设整改工作的指导意见》(公信安[2009]1429号)的规定,并结合本项目的实际情况,针对被测评的信息系统出具

《网络安全等级保护安全建设整改设计方案》。

四、项目实施及验收

项目实施过程中，投标人应遵循国家标准、行业标准。

4.1 项目实施要求

- 1) 提供的项目实施组织架构；
- 2) 提供详细的项目实施方案和计划进度说明书；
- 3) 提供详细、全面的人员培训计划和方案；
- 4) 项目实施完成后提供可靠的后期维护工作；
- 5) 严格按照双方确定的计划进度保质保量完成工作；
- 6) 规范项目实施过程中的文档管理；
- 7) 项目实施中要引入风险管理、质量管理、成本管理；
- 8) 本次测评项目工期为 60 天；

9) 为保障项目服务响应速度，投标人需在海南省本地部署等级保护测评师技术服务团队，测评师团队不得低于 15 人，投标人出具《人员本地部署承诺函》并盖公章。售后服务期间对于招标人的电话咨询和常规服务请求在 30 分钟内予以答复。

4.2 验收组织

成立由业主、投标人以及其他有关人员组成的验收小组，按照国家行业标准及招标文件要求负责对项目进行全面的验收。

- 1) 中标人必须提供给业主详细的项目验收方案；
- 2) 中标人必须书面通知业主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，此通知书需经业主认定后方可执行。

4.3 验收标准

- 1) 完成了本项目所有内容；
- 2) 提交符合公安机关要求的《网络安全等级保护全国信用信息共享平台（海南儋州）等级测评报告》和《网络安全等级保护安全建设整改设计方案》；
- 3) 提交项目实施阶段所有的项目文档。

(2) 商务要求

- 1、采购标的时间：2022 年 9 月

2、**采购标的地点：**采购人指定地点

3、**服务工期：**签订合同之日起1年

4、**交付地点（范围）：**采购人指定地点

5、**付款条件（进度和方式）：**

5.1 首付款：签订合同后15个工作日内支付合同款的50%。

5.2 尾款：项目通过竣工验收后支付合同款的50%。（具体以合同约定为准）。

6、**售后服务：**

1、**咨询服务**

投标人向招标人提供信息安全系统等级保护相关的政策、法律法规及技术要求和标准的咨询服务工作。

（1）**咨询服务时间：**自合同生效之日起，提供一年信息安全等级保护咨询服务。

（2）**咨询服务方式：**在咨询服务时间内，中标人将向招标人提供以下方式进行咨询服务方式。

服务方式具体如下：

序号	服务方式	服务响应
1	电话咨询服务	7*24 小时
2	QQ/微信在线咨询	5*8 小时
3	Email 咨询服务	1 小时
4	现场咨询服务	按需
5	应急咨询	按需

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。

中标人将针对整改过程中相关技术进行把关和提供相应的咨询，并保证在整改过程中确保响应，确保招标人可第一时间联系中标人相关工程师，解决相关问题。

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。

与此同时，在行业主管部门、公安部门、工信部门对招标人开展网络安全检查工作前，投标人应协助招标人做好安全检查前的自查工作，包括自查表、自查报告的编写等。

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。

5. E 包：商用密码应用安全性评估

(1) 技术要求如下：

1. 项目目标

项目的总体目标是：依据 GB/T 39786-2021 《信息安全技术信息系统密码应用基本要求》，对全国信用信息共享平台（海南儋州）二期项目信息系统开展密评工作，通过密评工作深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全水平奠定基础，推动国产密码应用工作的进一步落实，

保障和促进儋州市营商环境建设局信息化安全体系建设健康发展。同时，也指导儋州市营商环境建设局的信息安全保障体系建设，增强密码安全管理意识，促进安全管理水平的提高。

2. 项目内容

GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》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，出具《全国信用信息共享平台（海南儋州）密码应用安全性评估报告》，提出具有针对性的整改意见，并根据信息系统及安全防护措施的现状，提供其他安全服务，确保信息系统的安全运行。

3 项目需求

3.1 需求内容

1. 对全国信用信息共享平台（海南儋州）二期项目信息系统进行摸底、分析和梳理，提出详细的测评方案。

2. 针对全国信用信息共享平台（海南儋州）二期项目信息系统进行密码应用安全性评估，内容包括：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。

3. 完成密码应用安全性评估工作后，针对评估发现的问题，向儋州市营商环境建设局提交改进建议；儋州市营商环境建设局根据整改建议，对信息系统进行密码应用安全性整改，解决存在的问题。最后，整改后的结果，出具测评报告。

4. 服务保障工作：评估报告提交 1 年内，围绕评估发现的问题和针对性改进建议，测评服务机构应向儋州市营商环境建设局免费提供咨询服务。

3.2 服务清单

序号	评估对象	系统等级	系统描述
1	全国信用信息共享平台（海南儋州）	第三级	全国信用信息共享平台（海南儋州）是儋州市营商环境建设局的重要信息系统，承载了信用网站升级改造、信用联合奖惩系统、“双公示”等行政权力事项公示系统、信用信息分析系统、信用承诺管理系统、信用分级分

序号	评估对象	系统等级	系统描述
			类监管系统、政务诚信管理系统、合同履行管理系统、公共信用服务系统、“信易+”应用管理系统等子系统。

3.3 项目成果交付

1. 《全国信用信息共享平台（海南儋州）密码应用安全性评估测评方案》；
2. 《全国信用信息共享平台（海南儋州）密码应用安全性评估报告》；
3. 《全国信用信息共享平台（海南儋州）密码应用安全性评估整改建议》；

3.4 测评方案

按照商用密码应用安全性分类分级评估的要求，依据《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）要求及信息系统等级保护定级情况，进行评估，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

		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；
		重要数据传输	d) 应采用密码技术保证信息系统应用的重

		机密性	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 管理	了解并遵守密码相关法律法规和密码管理制度	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；

		度	
		建立密码应用岗位责任制度	<p>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:</p> <p>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;</p> <p>2) 对关键岗位建立多人共管机制;</p> <p>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;</p> <p>4) 相关设备与系统的管理和使用账号不得多人共用。</p>
		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。
	建设运行	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;
		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	d) 投入运行前应进行密码应用安全性评估,

		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. 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。

4.1. 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》。

4.2. 项目人员管理

★项目组人员均已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，现场实施人员需持证测评，必须为投标文件中的人员。（供应商需提供承诺函，若后续签订合同后供应商不按承诺函所述安排驻场人员的，将视为虚假应标）

4.3. 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。

4.4. 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。

4.5. 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；

(2) 商务要求

1、**采购标的时间**：2022 年 9 月

2、**采购标的地点**：采购人指定地点

3、**项目工期**：下达测评通知书后 90 天内交付《全国信用信息共享平台（海南儋州）二期项目信息系统密码应用安全性评估报告》。

4、**交付地点（范围）**：采购人指定地点

5、**付款条件（进度和方式）**：合同签订支付合同额的 35%，初验支付合同额的 45%，验收支付合同额的 15%，验收之日起满一年支付合同额的 5%。

6、售后服务：

6.1 供应商必须确保能建立一支具有一定服务能力的管理团队，并合理调配各岗位人员，保障服务工作相关岗位人员需要。

6.2 中标单位从全国信用信息共享平台（海南儋州）二期项目进场之日起 5 个工作日内要完成评估系统确定和测评方案编制。

6.3 中标单位需在全国信用信息共享平台（海南儋州）二期项目验收之前完成并提交密码应用安全性评估报告。

6.4 服务期间提供 7×24 服务响应，需要进行现场服务的，对海口市内，技术人员能够在 2 小时之内到达现场处理。

6.5 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。

6.6 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。

6.7 严格遵循操作规程，承担服务工作质量责任。

6.F 包：安全服务软件代码监测

(1) 技术要求如下：

一、项目服务内容

1 服务内容

代码审计（Code Audit）是由具备高技能和高素质的安全服务人员发起，检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。

代码审计服务的目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。信息安全问题时刻都有新的变化，新的攻击方法层出不穷，攻击者攻击的方向越来越侧重于利用软件本身的安全漏洞，例如 SQL 注入漏洞、跨站脚本漏洞、CSRF 漏洞等，这些漏洞主要由不良的软件架构和不安全的编码产生。

开展源代码审计能够降低源代码出现的安全漏洞，构建安全的代码，提高源代码的可靠性，提高应用系统自身安全防护能力。源代码安全检测能够帮助开发人员提高源代码的质量，从底层保障应用系统本身的安全，从早期降低应用系统的开发成本。

2 服务方法

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、C#、ASP、PHP、JSP、.NET 全面测试。

代码审计服务的主要内容包括但不限于：

- OWASP WEB TOP 10 漏洞
- Web 应用程序的权限架构
- Web 应用通信安全
- Web 应用框架安全性

代码审计参考依据：

代码审计服务将参考下列规范进行工作。

- CVE (Common Vulnerabilities & Exposures) 公共漏洞字典表
- OWASP OWASP_Testing_Guide_v3
- OWASP OWASP_Development_Guide_2005
- OWASP OWASP_Top_10_2010_Chinese_V1.0
- OWASP Mobile Security Project
- 信息安全技术 信息安全风险评估规范 (GB/T 20984-2007)
- 信息技术 信息安全管理实用规则 (GB/T19716-2005) (ISO/IEC17799:2000)
- 信息系统安全风险评估实施指南
- 设备、软件厂商公布的漏洞库

3 服务流程

代码审计服务主要分为四个阶段，包括测试前期准备阶段、检测阶段实施、复测阶段实施以及成果汇报阶段：

●前期准备阶段

在实施源代码安全检测工作前，负责项目实施的技术人员会和客户对源代码安全检测服务相关的技术细节进行详细沟通。由此确认源代码安全检测的方案，方案内容主要包括确认的源代码安全检测范围、最终对象、检测要求的时间等内容，客户签署源代码安全检测授权书。

在测试实施之前，会做到让客户对安全测试过程和风险的知晓，使随后的正式测试流程都在客户的控制下。

●检测实施阶段

在检测实施过程中，测试人员使用专业的代码安全检测工具扫描，完成初步的源代码安全检测测试执行工作。

然后由人工的方式进行确认和分析，对安全扫描的结果进行检测和验证，从

而对源代码安全漏洞进行定级，测试人员需整理源代码安全检测服务的输出结果并编制源代码安全检测报告，最终提交客户和对报告内容进行沟通。

●回归测试阶段

在经过初次源代码安全检测报告提交和沟通后，等待客户针对源代码安全检测发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给客户复测报告和对复测结果进行沟通。

●成果汇报阶段

根据初次源代码安全检测和二次复测结果，整理源代码安全检测服务输出成果，最后汇报项目领导。

4 服务成果

交付物资料包括不限于如下内容：

序号	名称	输出时间	备注
1	《代码审计服务方案》	启动阶段	
2	《源代码缺陷分析报告》	执行阶段	
3	《源代码缺陷溯源分析报告》	执行阶段	

二、项目服务范围

本次项目所涉及的服务对象如下：

序号	服务对象	备注
1	全国信用信息共享平台（海南儋州）二期项目定制软件的源代码	提供一次代码审计服务（含一次回归测试）

三、项目的实施要求

项目实施过程中，投标人应遵循相关标准和规范。

(一)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. 规范项目实施过程中的文档管理；

5. 项目实施中要引入风险管理、质量管理、成本管理；
6. 签署《保密协议》。

(二) 服务实施团队要求

1. 投标人须在投标文件中提供完整的服务实施团队名单及职责分工，所有实施人员必须属于投标人在册员工(以最近三个月社保缴纳证明为认定依据)，实施团队名单中所列人员的社保缴纳证明，复印件需在投标文件中提供，并加盖公章。

(三) 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，此通知书需经采购人认定后方可执行。

(四) 验收组织

成立由采购人、中标方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。

(五) 验收标准

- 1、完成了本项目的代码审计工作；
- 2、提交项目成果文档和过程文档。

(2) 商务要求

- 1、**采购标的时间：**2022 年 9 月
- 2、**采购标的地点：**采购人指定地点
- 3、**项目工期：**合同签订生之日起且具备代码审计服务实施条件（包括但不限于提供定制软件的源代码）后 60 个工作日内完成代码审计服务工作, 并输出服务成果。
- 4、**交付地点（范围）：**采购人指定地点
- 5、**付款条件（进度和方式）：**合同签订支付合同额的 35%，初验支付合同额的 45%，验收支付合同额的 15%，验收之日起满一年支付合同额的 5%。
- 6、**售后服务：**
 - 一、**咨询服务**
乙方向甲方提供代码审计相关的技术要求和标准的咨询服务工作。

1.1 咨询服务时间

自合同生效之日起，提供一年免费的咨询服务。

1.2 咨询服务方式

在咨询服务时间内，乙方将向甲方提供以下方式进行咨询服务方式。

服务方式具体如下：

序号	服务方式	服务响应
1	电话咨询服务	7*24 小时
2	QQ/微信在线咨询服务	5*8 小时
3	Email 咨询服务	5*8 小时
4	现场咨询服务	按需

1.3 咨询服务内容

1.3.1 代码审计建设整改咨询

按照代码审计对象安全总体方案要求，乙方将结合代码审计对象安全建设项目计划，根据网络安全相关标准和规定，对甲方代码审计建设或整改工作提供全面详细咨询。

二、服务要求

乙方将针对咨询过程中相关技术进行把关，并保证在咨询过程中确保 7*24 的响应，确保甲方可第一时间联系乙方相关工程师，解决相关问题；