

采购需求

一、项目概况

1. 采购单位：儋州市不动产登记中心；
2. 项目名称：提升不动产登记数据质量和共享应用能力项目；
3. 资金来源：财政资金；
4. 采购预算：¥2132300.00 元（大写金额：人民币贰佰壹拾叁万贰仟叁佰元整），包含本项目所有费用；其中分包信息如下：

包号	标包编号	标的名称	标包预算金额	标包最高限价
包 1	HNYH2023-27-0307（1）	提升不动产登记数据质量和共享应用能力	¥184.59 万元	¥177.65 万元
包 2	HNYH2023-27-0307（2）	硬件设备购置	¥17 万元	¥17 万元
包 3	HNYH2023-27-0307（3）	监理服务	¥6.64 万元	¥6.64 万元
包 4	HNYH2023-27-0307（4）	网络安全等级保护测评	¥5 万元	¥5 万元

二、项目采购标的

序号	包号	标的名称	计量单位	数量
1	包 1	提升不动产登记数据质量和共享应用能力	套	1
2	包 2	硬件设备购置	台	2
3	包 3	监理服务	项	1
4	包 4	网络安全级等级保护测评	项	1

三、技术商务要求

（一）包 1：提升不动产登记数据质量和共享应用能力

1、技术要求

（1）软件服务内容

1.1 服务内容

1.1.1 提升不动产登记数据质量和共享应用能力业务需求

为全面贯彻海南省自然资源和规划厅办公室关于做好提升不动产登记数据

质量和共享应用能力工作的通知，需规范录入新标准登记信息、实时上传新标准增量数据、日常新标准登簿日志的接入工作、全面完成数据整合汇交。通过分析《不动产登记数据库标准（2021 修订版）》标准，不动产登记信息系统、基础维护平台系统、新建商品房网上登记子系统需进行对应改造升级。

1.1.1.1 不动产登记信息系统改造升级

为实现规范录入新标准登记信息，需使不动产登记系统适应符合新的《不动产登记数据库标准（2021 修订版）》标准。

不动产登记系统是土地、房屋、海域、林权、农地承包等不动产的业务办理，经对现不动产数据库和新标准数据库结构分析，所有不动产的数据库表结构都有发生变化，因此不动产登记系统中的受理、审核、登簿、缮证、发证、归档、查询等模块都需做响应的修改。

本次提升不仅要符合新的不动产标准，同时还要满足登记数据实时上传，因此为了保证数据上传的实时性，需在不动产登记的登簿环节同步上传登记数据。将废弃当前数据上传机制，全新开发一种以接口服务的方式实现登记数据的实时上传。

完成增量数据比对、全库数据比对、销账管理功能模块的开发。

1.1.1.2 基础维护平台系统的改造升级

基础维护平台系统的楼盘建立、楼盘维护等功能都需做响应字段的增加、删除、修改。

自然幢属性结构变化

(1)增加：“楼幢代码”“楼幢坐落”“规划用途名称”“批准用途”“实际用途”字段。

(2)变更：“自然幢号”为“幢号”、“房屋结构”为“建筑结构”、“地上层数”字段类型为“Varchar”、“地下层数”字段类型为“Varchar”、“规划用途”字段长度为“3”。

(3)删除：“建筑物基本用途”字段。

逻辑幢属性结构变化

(1)增加：“幢标识码”“用途名称”“批准用途”“实际用途”字段。

(2)变更：“自然幢号”为“幢号”、“房屋结构1”为“建筑结构1”、“房

屋结构 2”为“建筑结构 2”、“房屋结构 3”为“建筑结构 3”、“房屋用途 1”字段长度为“3”、“房屋用途 2”字段长度为“3”、“房屋用途 3”字段长度为“3”、“地上层数”为字段类型“Varchar”、“地下层数”字段类型为“Varchar”。

层属性结构变化

- (1) 增加：“幢标识码”“逻辑幢号”字段。
- (2) 变更：“自然幢号”为“幢号”、“实际层”字段类型为“Varchar”。
- (3) 删除：“层套内建筑面积”“层阳台面积”“层分摊建筑面积”“层半墙面积”。

户属性结构变化

- (1) 增加：“宗地代码”“幢标识码”“用途名称”“批准用途”“实际用途”“房屋类型名称”“房屋性质名称”。
- (2) 变更：“自然幢号”为“幢号”、“房屋用途 1”字段长度为“3”、“房屋用途 2”字段长度为“3”、“房屋用途 3”字段长度为“3”。

1.1.3 新建商品房网上登记子系统

针对房屋所有权和房屋抵押权的首次登记、预告登记、转移登记的申请等功能，包括业务申请、受理列表、修改列表、证书管理。这些模块都需做相应属性字段的增加删除修改功能的升级。

1.1.2 洋浦数据加工迁移提升与系统更新需求

1.1.2.1 权籍调查数据迁移

权籍调查是不动产登记的基础工作，是不动产登记信息来源的主要渠道和登记依据。权籍调查数据迁移包括：地籍区数据、地籍区空间数据、地籍子区属性数据、地籍子区空间数据、宗地属性数据、宗地空间数据、土地承包林地属性数据、土地承包林地空间数据、楼盘属性数据、楼盘空间数据。按照儋州市不动产权籍调查数据库标准导入数据。

1.1.2.2 不动产登记数据迁移

洋浦的不动产数据入库后，儋州市不动产登记系统才能支持洋浦不动产发证。经调研分析洋浦的不动产信息包括国有建设用地使用权、集体建设用地使用权、农村宅基地使用权、海域使用权、林权、坐标、楼栋、户、房屋所有权、抵押、查封、预告等数据。将洋浦数据按照《不动产登记数据库标准（2021 修订版）》

标准入库。

1.1.2.3 电子扫描影像文件迁移

将洋浦原始影像数据在数据库中提取转换成文件后，再与不动产登记档案关联。

1.2. 工作量

需要完成不动产登记信息系统改造升级、基础维护平台系统的改造升级、新建商品房网上登记子系统升级。对洋浦不动产登记档案数据 78782 宗与调查数据 16376 宗进行整合加工和迁移，对洋浦不动产电子档案数据进行转换关联。

1.3. 成果要求

1.3.1 软件成果

完成不动产登记信息系统改造升级、基础维护平台系统的改造升级、新建商品房网上登记子系统升级。

1.3.2 数据成果

1.3.2.1 洋浦权籍调查数据：地籍区数据数据、地籍区空间数据、地籍子区属性数据、地籍子区空间数据、宗地属性数据、宗地空间数据、土地承包林地属性数据、土地承包林地空间数据、楼盘属性数据、楼盘空间数据。

1.3.2.2 洋浦不动产登记数据：国有建设用地数据、集体建设用地数据、农村宅基地数据、海域数据、林权数据、坐标数据、楼盘数据、户室数据、房屋数据、抵押数据、预告数据。

1.3.2.3 洋浦电子档案数据：文件形式电子档案。

1.3.3 文字成果

1.3.3.1 实施方案

1.3.3.2 技术细则

1.3.3.3 工作总结报告

1.4. 项目实施

不动产登记信息系统改造升级、基础维护平台系统的改造升级、新建商品房网上登记子系统升级要在现有平台基础上进行，升级过程不能影响正常不动产登记业务开展。

2、商务要求

(1) 合同履行期限：合同签订生效之日起 2 周内完成洋浦数据迁移，3 个月内完成主体工作成果，6 个月内完成全部工作，延期完成每日扣罚合同总价的 2% 的违约金，因甲方原因导致工期延长的除外。

(2) 服务地点：采购人指定地点。

(3) 付款方式

3.1 签订合同后，供应商完成人员进场，开展工作后，采购人依据供应商开具的有效发票，10 个工作日内向供应商支付合同金额 50%的预付款；

3.2 供应商按工期进度完成主体工作成果，采购人初步检查确认后，依据供应商开具的有效发票，10 个工作日内向供应商支付合同金额 40%的项目进度款；

3.3 供应商按工期进度全部完成合同约定内容，并通过验收后，采购人依据供应商开具的有效发票，10 个工作日内向供应商支付合同金额 10%的项目尾款。

(4) 验收标准：①满足国家、海南省、行业相关规范和标准的要求；②满足合同规定的相关要求；③达到了招标文件的采购需求。④达到了投标文件承诺的要求。⑤验收费用由中标供应商承担。

(5) 售后服务

实时解决系统运行中出现的问题，实时处理数据上传、数据比对出现的问题及时做好数据销账。

本项目包 1 为服务类项目，不设核心产品。

(二) 包 2：硬件设备购置

1、技术要求

1.1 硬件技术参数

序号	名称	技术参数和规格配置	单位	数量
一、安全设备				
1	入侵检测	<p>1、规格性能：</p> <p>①采用国产化 CPU 芯片及国产化操作系统。</p> <p>②内存：≥8GB，硬盘：≥512G 硬盘，网络层吞吐量≥3Gbps；并发连接≥300 万；冗余电源；标准 2U 设备；≥1 个 Console 管理口，≥1 个 HA 口，≥2 个 USB 口，≥2 个千兆电口，≥4 个千兆光口；3 年特征库升级服务，3 年硬件维保服务。</p> <p>2、功能参数：</p> <p>①支持旁路部署方式，提供数据收、协议分析、入侵逃避发现、流量监测能力；</p> <p>②▲提供最近 24 小时内网络发生的展示界面，包括对拒绝服务事件、扫描事件、蠕虫事件、木马病事件、网络整体状况等展示；（需提供功能截图证明并加盖厂商公章）</p> <p>③提供自定义弱口令规则的能力，使用户可以灵活定义网络内的弱口令条件；</p> <p>④提供威胁的实时展示能力，可以将引擎检测到的威胁在威胁展示界面进行实时显示，现实内容需全面丰富，包括：事件名称、攻击者 IP、被攻击者 IP、攻击发生时间、事件级别、流行程度、攻击类型；</p> <p>⑤提供网关 IP-MAC 地址绑定的功能识别 arp 地址欺骗攻击；</p>	台	1

序号	名称	技术参数和规格配置	单位	数量
		<p>⑥供完善的报表系统，支持面向安全结论的分析报表；报表需支持如下格式：HTML、PDF、EXCEL、WORD，所生成的报表可以自动发送到多个邮箱，能辅助用户查阅。</p> <p>⑦▲产品属于国产，符合信创目录内产品。</p> <p>⑧▲系统需具备对针对Web系统(包括浏览器、服务器)的攻击具备检测能力：SQL注入（包括各种变形）、XSS（包括存储式XSS、反射式XSS）及其各种语法变形、Webshell、网页挂马、语义变形、编码等环境下的精确检测能力（需提供功能截图证明并加盖厂商公章）</p> <p>⑨能够对缓冲区溢出、网络蠕虫、网络数据库攻击、木马软件、间谍软件等各种攻击行为进行检测（需提供功能截图证明并加盖厂商公章）</p> <p>⑩系统提供的攻击特征不应少于3600条有效最新攻击特征，并且根据协议类型、安全类型、流行程度、影响设备等方式做有效分类（需提供功能截图证明并加盖厂商公章）</p> <p>⑪▲具有自主研发入侵检测方法和装置（需提供国家第三方机构认证的技术证明文件并加盖厂商公章）</p>		
2	日志审计	<p>1、规格性能：</p> <p>①采用国产化CPU芯片及国产化操作系统。</p> <p>②内存：≥8GB，硬盘：≥2T 硬盘，日志处理性能（平均）≥3000EPS；单交流电源；标准1U设备；≥1个Console管理口，≥2个USB口，≥6个千兆电口，≥4个千兆光口；≥2个接口扩展槽；≥40个日志审计对象授权许可，3年硬件维保服务。</p>	台	1

序号	名 称	技术参数和规格配置	单位	数量
		<p>2、功能参数：</p> <p>①提供网络设备、安全设备与系统、主机、中间件、数据库、存储、应用和服务在内的多种审计数据源的日志采集，并且提供日志过滤归并功能提高日志采集能力；</p> <p>②▲支持对国内主流国产化数据库进行日志数据采集，包括武汉达梦、人大金仓、南大通用、神州通用等；支持动态表名模式进行数据库采集，能按照时间或者数字的规则动态每天递增采集日志表；（需提供功能截图证明并加盖厂商公章）</p> <p>③▲支持日志加密压缩传输，支持加密压缩方式转发，支持定时转发；（需提供功能截图证明并加盖厂商公章）</p> <p>④支持多种告警方式和告警动作，包括弹出提示框、播放警示音、发送邮件、发送 SNMPTrap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送 Syslog 等；</p> <p>⑤支持三权分立，包括系统管理员、安全审计员和安全保密管理员；</p> <p>⑥▲产品属于国产，符合信创目录内产品。</p> <p>⑦支持自定义事件搜索条件，并作为检索策略保存，以树形结构进行组织，形成一个搜索分析策略树（需提供截图证明并加盖公章）</p> <p>⑧内置不同审计分析场景，包括各种实时分析场景、历史统计场景、实时统计等。并支持支持自定义审计场景。</p> <p>⑨支持三权分立，包括系统管理员、安全审计员和安全保密管理员；</p> <p>⑩▲具有自主研发一种海量日志关联分析方法及系统（需提供国家第三方机构认证的技术证明文件并加盖厂商公章）</p> <p>⑪产品须提供由中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，认证级别为增强级，（需证书复印件并加盖厂商公章）</p>		

本项目包 2 的核心产品为：入侵检测、日志审计

1.2 工作量

完成硬件安装、测试和试运行。并申请通过二级等保。

1.3 成果要求

硬件运行无问题，通过二级等保。

1.4 项目实施

安装入侵检测、日志审计。

2、商务要求

(1) 合同履行期限：合同签订生效之日起 1 个月内安装部署完成，并于 1.5 个月内完成全部工作提交验收。

(2) 服务地点：采购人指定地点。

(3) 付款方式

3.1 签订合同后，供应商完成人员进场，开展工作后，采购人依据供应商开具的有效发票，10 个工作日内向供应商支付合同金额 50%的预付款；

3.2 供应商按工期进度完成主体工作成果，采购人初步检查确认后，依据供应商开具的有效发票，10 个工作日内向供应商支付合同金额 40%的项目进度款；

3.3 供应商按工期进度全部完成合同约定内容，并通过验收后，采购人依据供应商开具的有效发票，10 个工作日内向供应商支付合同金额 10%的项目尾款。

(4) 验收标准：①满足国家、海南省、行业相关规范和标准的要求；②满足合同规定的相关要求；③达到了招标文件的采购需求。④达到了投标文件承诺的要求。⑤验收费用由中标供应商承担。

(5) 售后服务

硬件服务：符合国家三包政策，安排技术业务经验丰富的员工负责，实时解决硬件运行中出现的问题，三年内免费上门维修。

(三) 包 3 : 监理服务

1、技术要求

1.1 项目建设内容

1.1.1 提升不动产登记数据质量和共享应用能力

- (1) 不动产登记信息系统改造升级
- (2) 基础维护平台系统改造升级
- (3) 新建商品房网上登记子系统改造升级

1.1.2. 洋浦数据加工迁移提升与系统更新

1.2 监理服务内容

(1) 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”,对本项目提升不动产登记数据质量和共享应用能力:(1) 不动产登记信息系统改造升级。(2) 基础维护平台系统改造升级。(3) 新建商品房网上登记子系统改造升级。及洋浦数据加工迁移提升与系统更新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。

1.3 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像；

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施工工序和项目的影晌程度，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/TG22239-2019），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/TG22239-2019），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) 监理单位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。

1.4 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证书、软件测试工程师证书、软件设计工程师证书、咨询工程师登记证书，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) 合同履行期限：自签订合同之日起，至项目完成竣工验收止。

(2) 项目实施地点：采购人指定地点（海南省内）。

(3) 付款时间、方式及条件（具体金额及支付方式以合同为准）：

预付款：签订合同后 30 个工作日内，甲方支付乙方合同总金额的 30%；

初步验收款：项目初步验收合格后 15 个工作日内，且未发生任何违约行为，甲方向乙方支付合同总金额的 60%；

最终验收款：项目竣工验收合格后 15 个工作日内，且未发生任何违约行为，甲方向乙方支付合同总金额的 10%。

(4) 验收方法及标准：按本招标文件和投标文件的内容及国家、地方和行业的相关政策、法规实施，验收费用由中标供应商承担。

本项目包 3 为服务类项目，不设核心产品。

(四) 包 4: 网络安全等级保护测评

1、技术要求

(1) 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、系统定级情况如下

序号	拟测评系统名称	依据级别
1	不动产统一登记发证子系统	拟二级(S2A2G2)

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》GB/T 22240-2020;
7. 《信息安全技术 信息安全风险评估规范》GB/T 20984-2022。

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等级测评，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	拟测评系统名称	依据级别
1	不动产统一登记发证子系统	拟二级(S2A2G2)

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》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
	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	

		到表单
--	--	-----

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 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。 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	《测评方案》的测评指标部分
三、测评	确定每个测评对象对应的每个测评指标的	《测评方案》

内容确定	测评方法	的 单项测评实施部分
	确定实施测评的单项测评内容	
四、工具测试点确定	<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> <p>渗透测试工具；</p> <p>SQL 注入验证检查工具；</p> <p>在线数据库安全检查工具。</p>	《测评方案》的 的工具测试方法及内容部分
	五、测评指导书开发	

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	<p>《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;</p> <p>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>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>
	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	
	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	
	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	

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存在情况	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

	根据各对象的单项符合程度得分, 计算安全控制点得分	
	根据安全控制点得分, 计算安全层面得分	
	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	
5. 安全问题 风险分析	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	测评报告的安全问题 风险分析部分
	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	
	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”	
6. 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
	计算定级对象综合得分, 形成等级测评结论, 形成等级测评结论	
7. 测评报告编制	概述测评项目情况, 整理前面几项任务的输出/产品	经过评审和确认的被测定级对象等级测评报告
	针对被测定级对象存在的安全隐患, 提出处置建议	
	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

投标人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

2、商务要求

- (1) 项目实施地点：儋州市；
- (2) 服务期限：自签订合同之日起 1 年；

(3) 付款方式：合同生效之日起 30 个工作日内，甲方凭乙方开具的等额、合法、有效发票向乙方支付合同金额的 30 %；项目完成后乙方出具正式等级保护测评报告起 30 个工作日内，甲方凭乙方开具的等额、合法、有效发票向乙方支付合同金额的 60%；项目竣工验收后，甲方凭乙方开具的等额、合法、有效发票向乙方支付合同金额的 10%。

- (4) 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) 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) 本次测评项目工期为 60 天；

7) 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 8 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，紧急服务请求在 4 小时内到达招标人现场。

8) 根据招标人项目的实际情况，本次项目测评组人员至少安排 1 名高级测评师、3 名中级测评师和 4 名初级测评师开展等级保护测评工作。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最近连续三个月社保缴纳证明和《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。

4.2 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《网络安全等级保护等级测评报告》；
- 3) 提交项目实施阶段所有的项目文档；
- 4) 验收费用由中标供应商承担。

本项目包 4 为服务类项目，不设核心产品。