项目需求

一、基础运维服务

扬州市房建市政交易7.0系统主要涉及其包含的交易业务系统、不见面开标系统、评标系统及远程协调系统等。

1、日常巡检：制定巡检计划并做好巡检工作，按日、周、月、季、半年及年度或任意需求时间段提供运维报告，包括日常巡检功能可用性和服务有效性检查；及时发现并处理各软件系统运行中出现的问题；现有功能的适应性改进（不涉及系统架构）。 7.0系统日常运行的安全巡检服务，包括但不限于系统发布内容的检查监控；系统目录及数据的异地或异机备份的安全、分析系统日志和统计信息，预防问题的发生；产品补丁的安装、数据库空间监控、规划及管理、数据库常见问题的分析、诊断及解决；数据库性能的评估、监测和调整；系统资源的监控及管理、数据库安全及用户的管理。

2、系统功能维护：针对系统功能提供日常维护服务，确保系统平台业务处理能力、开标评标能力、远程协调能力以及违规预警能力，保持系统对外服务接口正常运行，保证整个系统平台功能完整、运行安全稳定。

3、故障排除：运维方详细记录每次故障时间、地点、故障现象、处置过程、处置结果和处置时间等内容，需经中心签字认可，并作为服务验收依据。对于不影响系统整体的运行的故障，应当在1小时内排除；对系统部分功能无法正常使用、或数据错误、但主要业务系统仍可正常工作的故障，应当在2小时内排除；系统停止运行或导致信息系统运行性能下降且无法保证业务正常开展的，应当4小时内排除；发生重大宕机事件或业务系统发生重大故障需重新部署系统的故障，应当24小时内排除。

4、数据维护：依据国家、省反馈的数据归集存在问题及时对相应数据项进行修改、完善和补推；按照系统的实际配置情况，制定数据备份计划，为数据恢复提供完整的依据；数据库及数据平台项目均应建立异地容灾备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复；各容灾备份系统应具有一定兼容性，在特殊情况下各系统间可互为备份。

5、驻场运维：现场常派3名以上驻场技术人员，要求对7.0系统相当熟悉。现场运维人员提供现场服务，负责7.0系统的现场日常维护更新工作，保障系统的正常稳定运行；需对项目运维日常查看保障、制定相关实施计划，保证计划实现；组织、指导后方团队远程开展运维工作；负责依据如巡视、审计等要求组织实施开展数据准备工作；发现、解决问题，提出解决办法和建议；日常跟踪不见面开标系统并及时处置延时、卡顿、断针等问题；对中心信息化需求派单开展评估、制定计划及指导开发团队实施；负责全市各分中心系统问题的紧急现场处置应等。

6、远程运维支持：出于流程规范以及平台安全、释放现场交付工程师的工作压力，现场不接触代码，配备远程运维小组，配合现场人员，解决问题，保障系统稳定运行。并可以提供相关安全服务、系统测试，以及其他优化建议。

7、日常咨询服务：现场运维人员需为各方主体用户提供日常咨询、技术指导与服务，服务包含：现场咨询、工作电话咨询，提供的服务需面向代理机构、交易中心及其他日常咨询、技术指导与服务。组建客服团队提供400专业咨询渠道，提供5\*8小时服务，主要包括业务系统咨询和日常操作问题处理，面向代理机构、交易中心及其他相关主体提供日常咨询与技术指导服务，保障招投标活动顺利推进。

二、功能研发、系统对接服务

1、依据省数据局、省公共资源交易中心2025年工作要点中部署的涉建设工程领域的信息化推进目标，协助市公共资源交易中心制定扬州市公共资源交易信息化实施方案，配备相应技术力量人员按时序推进7.0系统相关信息化建设工作。

2、负责完成为落实国家、省各级各界部门关于推进优化营商环境和改革发展重大、重点工作而涉及到的7.0系统全新功能研发、部分模块功能优化、第三方平台接口开发对接以及联调测试等突击性工作任务。

3、依据市公共资源交易中心落实行业监管部门、执纪执法监督部门以及各方市场主体关于交易系统功能合理化建议的建设需求，进行工作量、时长、风险评估，配备相应技术力量，根据中心“派单”要求完成7.0系统相应功能研发与完善工作。

4、负责完成因中心其他相关创新工作（如“AI+公共资源交易”）开展而涉及到7.0系统必要的相关改造与适配工作。

5、负责完成其他在开展日常建设工程交易招投标活动过程中，中心提出的7.0系统改造、优化、提升需求。

三、应急服务

1、现场应急服务：在出现安全事件后，驻场人员负责对计算机系统和网络安全事件的处理提供技术支持和指导，处理过程应遵循正确的流程，采取正确快速的行动作出响应，尽最大可能收集事件相关信息，明确事件类别，确定事件来源，保护证据，以便缩短应急响应时间。

2、应急处置：（1）检查威胁造成的结果，评估事件带来的影响和损害：如检查系统、服务、数据的完整性、保密性或可用性，检查攻击者是否侵入了系统，以后是否能再次随意进入，损失的程度，确定暴露出的主要危险。（2）抑制事件的影响进一步扩大，限制潜在的损失与破坏。（3）通过对有关恶意代码或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。（4）清理系统，恢复数据、程序、服务。把所有被攻破的系统和网络设备彻底还原到它们正常的任务状态。

3、备份与恢复策略：必须建立完整的系统备份档案，保证宕机时能将系统及时恢复至包括相关软件配置的原有状态。根据应用的实际情况，列出所有相关数据的连接关系，以便制定详细的应用系统数据备份计划，为数据恢复提供完整的依据。

4、应急措施：应针对黑客攻击事件、病毒事件、软件系统遭破坏性攻击、系统存在严重BUG造成业务操作失误、数据错误、数据库安全、数据库中数据被大面积非法篡改或删除等情况制定紧急处置预案，并在发生重大安全事件时予以启动应急措施，保障7.0系统安全稳定运行。

5、总结报告：回顾并整理已发生事件的各种相关信息，尽可能地把所有情况记录到文档中。发生重大信息安全事件的，应当在事件处理完毕后将处理结果备案。

6、安全培训：组织协调组和数据管理组应加强对系统突发事件应急的宣传教育工作，定期或不定期地组织有关部门及保障人员进行技术培训和应急演练，保证应急预案的有效实施，不断提高应对系统突发事件的能力。