北京市体育彩票管理中心

实体店综合业务平台采购需求

## 一、项目概述

目前随着北京市体育彩票销售规模的不断扩大，为进一步规范渠道管理业务流程，整合和管理渠道信息，进而提升对实体销售渠道的管理运营效率和质量，北京市体育彩票管理中心计划采购实体店综合业务平台开发运维服务，并与中心已有的系统进行数据集成，为中心提供数字化、系统化、智能化的实体店管理及服务平台。

## 二、项目名称

实体店综合业务平台服务

## 三、项目预算

项目采购金额25.404万元，分两次列支，支出比例为：50%、50%。

支付项目尾款前，服务商需要提供中标价的10%的《履约保函》，有效期不少于1个月。

## 四、项目服务期限

签订合同之日起4个月

## 五、项目服务要求

### （一）系统功能需求

1、业务流程管理

支持北京体彩中心现有实体店征召、变更等业务办理，对业务进行规范化流程管理，包括但不限于实体店新增、挪址、撤销、升级、停开机、属性变更、异常票申报、故障报修等。

系统需支持提交流程申请、处理和审批流程，同时支持部分流程进行批量申请、批量审批等操作。系统支持待处理人员查看自己的流程待办事项。支持业务干系人随时查看流程进度、流程详情及流程审批记录，进行流程跟踪。

可根据北京体彩中心业务需要，对流程进行调整优化。包括但不限于对流程发起人、审核人的变更，流程节点的增减，表单内容的变更，流程审批记录的呈现等。

2、渠道管理

支持渠道相关业务信息的管理，包括实体店管理、代销者管理。

实体店管理：对实体店相关信息进行管理，支持查询实体店信息，包括实体店基本信息、代销者信息、专管员信息、终端信息、资产信息、实体店照片等；支持在地图展示门店分布、门店地图定位、门店检索等功能。支持拥有高级管理权限的用户对实体店信息进行新增、编辑、删除、导入、导出等操作。

代销者管理：对代销者相关信息进行管理，支持查询代销者信息，包括代销者基本信息、代销实体店信息、代销者照片等；支持拥有高级管理权限的用户对代销者信息进行新增、编辑、删除、导入、导出等操作。

3、专管员管理

门店分配：支持查询专管员管辖门店信息，支持管理人员调整专管员管辖门店范围。

4、巡检调研

支持按店或区域发布巡检任务，支持对不同对象发布调研问卷，可对巡检、调研流程进行跟踪管理，对数据进行汇总统计。

5、报表管理

支持根据不同部门的需求对业务流程数据进行统计、展示，支持导出相应的流程工作报表、流程响应时间报表、故障维修记录报表等。

6、消息管理

支持在业务流程中自动生成短信发送用户流程待办提醒、流程处理结果等信息。

7、用户管理

系统用户包括体彩中心人员、专管员、代销者及系统管理员。

支持对系统用户查询及管理功能。包括用户账户信息、个人基本信息、密码及状态的管理。

支持对系统用户设置角色及权限，不同角色可设置不同模块的访问、管理及流程审批权限。确保不同角色之间的权限分离和职责明确。

8、多平台支持

系统支持PC端和手机端。

### （二）技术支持

1、团队驻场要求

供应商需根据中心要求，安排项目团队驻场北京市体育彩票管理中心现场沟通需求和驻场项目实施。若因为特殊原因无法长期驻场的，需随时根据中心要求，在30分钟内到现场提供技术服务。

2、应急响应

供应商需提供7\*24小时的电话技术支持，出现问题或故障需要后台系统处理或远程处理，通过电话或远程协助等方式解决问题的响应时间不超过1小时。无法远程解决需到现场进行问题处理的响应时间不超过2小时，完成故障修复保证系统功能正常使用的时间不超过1个工作日，故障修复后2个工作日内提供故障报告。

3、培训要求

供应商需在每次系统更新前提供更新说明和操作说明，遇重大版本更新，需要时提供培训服务，培训方式不限于现场培训、线上培训。

### （三）运维需求

1、设备维护

供应商需提供系统研发及运维工作，所使用的软硬件设备的相关搭建、运维、更新工作。

2、设备安全

实体店综合业务平台部署的线上环境具有WAF、防火墙、入侵检测等安全防护和安全监测的安全设备。

（1）WAF防火墙

针对实体店综合业务平台进行有效的WAF防护。保障系统免受已知、未知攻击。

（2）抗拒绝服务系统

支持在IPv4、IPv6及两者混合环境中，防护各类DDoS攻击。提供应对大流量DDoS攻击的云地混合防护。

（3）网络入侵防护系统

能够具备紧急漏洞24小时响应能力;采用恶意文件检测技术，增强文件防护能力;为应对高级威胁，联动沙箱实现未知威胁的检测;协同威胁情报系统，提供千万级的恶意IP、恶意URL及C&C情报库，提供秒级防护能力。

3、系统服务器管理

建立服务器档案，对数据进行定期备份，对核心服务器进行备件，对相关服务器进行定期巡检，每月提供服务器巡检报告包括记录变化情况，CPU、内存、硬盘、电源报警状况、网线联通状态等。

4、安全漏洞扫描

每年提供一次专业第三方检测公司出具的无安全漏洞的系统漏洞扫描报告。

5、遭遇攻击后进行安全监测

如网站遭遇黑客攻击、病毒或因为其他第三方原因导致系统无法使用，供应商应在12小时内恢复正常，同时在问题解决后承担专业网络公司进行安全监测的相关费用。

6、数据及个人信息安全

系统需满足《中华人民共和国个人信息保护法》和《中华人民共和国数据安全法》的相关要求，针对个人信息等敏感数据采用加密存储、信息遮掩等有效措施进行安全防护，包括但不限于身份证号、手机号、银行卡号等信息，未经采购人授权，不得将任何数据提供给第三方。

7、其他运维需求

供应商需要及时响应我中心的需求变化，并根据需求及时安排系统的变更，包括但不限于软硬件、安全性等方面的需求变更。整个过程需要接受我中心的监督和管理。供应商需要在我中心的安全月及重保期响应我中心的要求，及时做好安全风险排查，并安排相应人员进行值守。供应商需要针对每次重大事件提供相应的总结报告。

### （四）部署实施需求

供应商需要自合同签订之日起10个工作日内完成与原供应商的工作交接。如果涉及原系统升级改造或采用全新系统，供应商需确保项目运营的延续性与稳定性，以及历史数据的完整性和连续性。

### （五）版本更新要求

为了确保系统的稳定性和持续优化，供应商需根据中心需求对系统进行持续化更新，项目上需采用敏捷的方式进行迭代开发交付，根据系统各功能的轻重缓急梳理优先级，提交项目迭代需求和计划。经中心确认后，快速完成开发和部署实施。每次迭代周期不超过1个月。

### （六）验收要求

每次项目迭代上线后，双方将对本次项目迭代中的需求点进行验收。如在验收过程中发现有需求点未达到预期标准，供应商需根据整改意见进行调整，在中心规定的时间内完成整改，并重新提交验收。整体项目结束后，供应商需要向我中心提供项目服务报告用于项目验收。