电子卖场竞价采购需求

项目名称：长沙市智能交通管理系统（第三期续建）项目等保测评项目

项目单位：长沙市公安局交通警察支队

编制时间：2022 年 8 月

2022 年 8 月

一、项目概况

长沙市智能交通管理系统（第三期续建）项目在现有道路网络条件下，以合理组织规划交通流，完善道路交通管理设施，加强与提高交通参与者的现代化交通意识为基础，以道路交通有序、畅通、安全以及交通管理规范服务、快速反应和决策指挥为目标，在一二三期项目的基础上，以大数据为驱动，以科技创新为动力，以信息技术为依托，完善建设集高新技术应用为一体的适合于本地区道路交通特点的、具有高校快捷的交通数据采集处理能力、决策能力和组织协调指挥能力的智能交通管理系统，实现交通管理指挥现代化管理数字化、信息网络化、办公自动化、最终实现三个服务的目标，即服务于交通参与者，提高道路的通行效率、服务于交通管理者，提升警力的指挥效率、服务于政府决策者，提供专业的技术支撑。

项目建设内容包括4个前端感知系统扩容、2个前端按照系统新建、5个平台升级、网络和安全建设、服务器和存储建设、3个配套工程及信号调优服务项目。其中升级扩容4个前端感知系统是指智能交通信号控制系统、高清电子警察系统、高清电视监控系统、三级分控系统；2个新建前端感知系统是指行人、电动车交通违法智能管理系统、人脸识别应用管理系统；5个平台是指大联合指挥调度管理平台、视频联网共享平台、道路交通运行指数平台、大联合情报信息平台、公安集成指挥平台。

为保障长沙市智能交通管理系统（第三期续建）项目平稳上线运行，依据《中华人民共和国网络安全法》、国家有关等保测评标准规范、长沙市数据资源管理局关于项目竣工验收的相关要求，结

合项目招标文件、合同等文件资料，聘请第三方专业等保测评机构为长沙市智能交通管理系统（第三期续建）项目相关信息系统建设过程提供安全整改咨询服务、提供相应的安全整改加固建议方案、开展等级保护整改回归测试，并通过测评定级，取得相关系统等级保护备案证明，获得符合长沙市数据资源管理局认可的测评报告。通过等级保护测评和整改加固工作，进一步提升长沙市智能交通管理系统（第三期续建）项目相关信息系统安全保障能力与水平，确保我支队核心业务信息系统的风险可控、可管与可靠运行。

二、采购方式

湖南省电子卖场竞价采购

三、采购控制价

人民币叁拾伍万元整（¥350000.00）

四、采购标的

序号	标的名称	计量单位	数量	是否进口
1	长沙市智能交通管理系统（第三期续建）项目等保测评项目	项	1	否

五、投标人资格要求

1. 投标人须具有公安部第三研究所颁发的《网络安全等级测评与检测评估机构服务认证证书》，提供证书复印件，原价备查。

2. 投标人须具备公安部第一研究所网防安全服务中心授牌，提供证书复印件，原件备查。

3. 投标人实施团队中有成员曾在全国网络与信息安全管理职业技能大赛获奖，提供实施团队在投标单位2022年1月至6月的社保证明和获奖证书复印件，原件备查。

4. 投标人近五年来未收到国家（及省级）网络安全等级保护协调小组办公室警告、处罚、整改，提供相关证明材料或承诺函。

5. 投保人必须同时具有中国网络安全审核技术与认证中心颁发的信息安全服务资质认证证书—信息安全风险评估资质、信息系统安全运维资质、信息安全应急处理服务资质，提供证书复印件，原价备查。

六、技术参数

（一）总则

1. 技术参数中各条款所提出的各项要求，是本次信息系统安全等级保护测评依据，投标人应根据本文件中的相关说明和要求提供方案。

2. 投标人在测评方案书中，对能提供的信息系统安全等级保护测评进行说明，可根据具体情况在项目方案中提出建议，并附详细资料和说明。

3. 投标人应对提供信息系统安全等级保护测评时所使用的设备及软件保证拥有设备软硬件的知识产权和所有权，并对所涉及的专利、知识产权等法律条款承担义务，采购人对以上问题不承担任何法律责任。

（二）依据政策及标准

投标人应依据国家相关政策标准开展工作，依据标准包括但不

限于如下国家政策标准:

- 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）;
- 《信息安全等级保护管理办法》（公通字〔2007〕43 号）;
- 《信息安全技术 信息系统安全等级保护实施指南》;
- 《信息安全技术 信息系统安全等级保护定级指南》（GBT 22240-2020）;
- 《信息安全技术 网络安全等级保护基本要求》（GBT 22239-2019）;
- 《信息安全技术 网络安全等级保护测评要求》（GBT 28448-2019）;
- 《信息安全技术 信息安全风险评估规范》（GB/T 20984—2007）;

（三）测评范围

根据相关文件及标准要求对长沙市智能交通管理系统（第三期续建）项目所建的信息系统开展等级保护测评，内容包括信息系统安全等级保护测评服务。

信息系统安全等级保护测评包含以下系统:

序号	系统	级别	备注
1	大联合指挥调度管理平台	三级	含行人、电动车交通违法智能管理系统、智能网联可视化运管模块、高清电子警察系统等

2	视频联网共享平台	三级	含高清电视监控系统
3	道路交通运行指数平台	三级	/
4	公安集成指挥平台	三级	/
5	人脸识别应用管理系统	三级	/

（四）测评内容

依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）要求，对信息系统进行等级测评，找出系统与国家标准要求之间的差距，对存在的风险进行评估，并出具《信息安全等级测评报告》和《安全建设整改方案》。测评内容涵盖:

1. 安全物理环境

安全物理环境测评将通过访谈和检查的方式评测信息系统的物理安全保障情况。主要涉及对象为机房。

在内容上，物理安全层面测评实施过程涉及 10 个安全子类:

序号	安全子类	测评指标描述
1	物理位置的选择	通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。
3	防盗窃和防破	通过访谈物理安全负责人，检查机房内的主要设备、

	坏	介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。
5	防火	通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。
6	防水和防潮	通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信息系统是否采取必要措施来防止水灾和机房潮湿。
7	防静电	通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。
9	电力供应	通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。
10	电磁防护	通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。

2. 安全通信网络

安全通信网络测评将通过访谈、检查和测试的方式评测信息系

统的网络安全保障情况。主要涉及对象机房的网络设备、网络安全设备以及网络拓扑结构等三大类对象。

在内容上，通信网络安全层面测评过程涉及3个工作单元:

序号	安全子类	测评指标描述
1	网络架构	通过访谈网络管理员，检查网络拓扑情况、核查核心交换机、路由器，测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	通信传输	通过访谈网络管理员，检查各硬件设备传输过程中是否采用加密技术。
3	可信验证	通过访谈网络管理员，检查各硬件设备传输过程中是否采用可信验证技术。

3. 安全区域边界

安全区域边界测评将通过访谈、检查和测试的方式评测信息系统的边界防护。

在内容上，安全区域边界测评实施过程涉及6个安全子类:

序号	安全子类	测评指标描述
1	边界防护	通过访谈网络管理员，查看边界设备防护措施。
2	访问控制	通过访谈网络管理员，查看边界设备的访问控制策略。
3	入侵防范	通过访谈网络管理员，查看各个关键网络节点的防入侵措施。
4	恶意代码防范	通过访谈网络管理员，查看各个关键网络节点恶意代

	和垃圾邮件防范	码防范措施。
5	安全审计	通过访谈网络管理员，查看边界设备的日志审计策略和记录。
6	可信验证	通过访谈网络管理员，查看边界设备是否采用可信验证技术。

4. 安全计算环境

安全计算环境测评将通过访谈、检查和测试的方式评测信息系统的应用安全保障情况。

在内容上，安全计算环境测评实施过程涉及 11 个工作单元，具体如下表:

序号	安全子类	测评指标描述
1	身份鉴别	检查信息系统网络设备、安全设备、服务器、数据库和应用系统的身份标识与鉴别功能设置和使用配置情况; 检查应用系统对用户登录各种情况的处理，如登录失败处理、登录连接超时等。
2	访问控制	检查网络设备、安全设备、服务器、数据库和应用系统的访问控制功能设置情况，如访问控制的策略、访问控制粒度、权限设置情况等。
3	安全审计	检查网络设备、安全设备、服务器、数据库和应用系统的安全审计配置情况，如覆盖范围、记录的项目和

		内容等; 检查应用系统安全审计进程和记录的保护情况。
4	可信验证	检查计算设备的系统引导程序、系统程序、重要配置参数和应用系统程序等是否可以进行可信验证，并检测可信验证受到破坏时进行报警。
5	入侵防范	检查网络设备、安全设备、服务器、数据库和应用系统入侵防范，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。
6	恶意代码防范	检查网络设备、安全设备、服务器、数据库和应用系统恶意代码防范措施。
7	数据完整性	检查网络设备、安全设备、服务器、数据库和应用系统的通信完整性保护情况。
8	数据保密性	检查网络设备、安全设备、服务器、数据库和应用系统的通信保密性保护情况。
9	数据备份和恢复	检查网络设备、安全设备、服务器、数据库和应用系统的关键信息备份情况。
10	剩余信息保护	检查网络设备、安全设备、服务器、数据库和应用系统。
11	个人信息保护	检查系统收集个人信息和使用个人信息的情况。

5. 安全管理中心

在内容上,安全管理中心层面测评实施过程涉及 4 个工作单元,具体如下表:

序号	安全子类	测评指标描述
1	系统管理	通过访谈系统管理员，对系统的资源和运行配置进行配置、控制和管理是否全由系统管理员进行操作。
2	审计管理	通过访谈安全审计员，是否对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
3	安全管理	通过访问安全员，对系统的安全策略进行配置，包括安全参数的设置、主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略是否全由安全员进行操作。
4	集中管控	通过访谈安全员，对分布在网络中的安全设备或安全组件进行管控，对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测、对分散在各个设备上的审计数据进行收集汇总和集中分析，对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理，对网络中发生的各类安全事件进行识别、报警和分析的情况。

6. 安全管理制度

安全策略和管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。

在内容上，安全管理制度测评实施过程涉及4个工作单元，具体如下表:

序号	安全子类	测评指标描述
1	安全策略	通过访谈安全主管，检查有关管理制度文档和重要操作规程等过程，测评信息系统管理制度在内容覆盖上是否全面、完善。
2	管理制度	通过访谈安全主管，检查有关制度制定要求文档等过程，测评信息系统管理制度的制定和发布过程是否遵循一定的流程。
3	制定和发布	通过访谈安全主管，检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。
4	评审和修订	通过访谈安全主管，检查管理制度评审记录等过程，测评信息系统管理制度定期评审和修订情况。

7. 安全管理机构

安全管理机构测评将通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

序号	安全子类	测评指标描述
1	岗位设置	通过访谈安全主管，检查部门/岗位职责文件，测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。

2	人员配备	通过访谈安全主管，检查人员名单等文档，测评信息系统各个岗位人员配备情况。
3	授权和审批	通过访谈安全主管，检查相关文档，测评信息系统对关键活动的授权和审批情况。
4	沟通和合作	通过访谈安全主管，检查相关文档，测评信息系统内部部门间、与外部单位间的沟通与合作情况。
5	审核和检查	通过访谈安全主管，检查记录文档等过程，测评信息系统安全工作的审核和检查情况。

8. 安全管理人员

安全管理人员测评将通过访谈和检查的形式评测机构人员安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

在内容上，人员安全管理测评实施过程涉及 4 个工作单元，具体如下表:

序号	安全子类	测评指标描述
1	人员录用	通过访谈人事负责人，检查人员录用文档等过程，测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。
2	人员离岗	通过访谈人事负责人，检查人员离岗安全处理记录等过程，测评信息系统人员离岗时是否按照一定的手续

		办理。
3	安全意识教育和培训	通过访谈安全主管，检查培训计划和执行记录等文档，测评是否对人员进行安全方面的教育和培训。
4	外部人员访问管理	通过访谈安全主管，检查有关文档等过程，测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

9. 安全建设管理

安全建设管理测评将通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。

在内容上，系统建设管理测评实施过程涉及10个工作单元，具体如下表:

序号	安全子类	测评指标描述
1	定级和备案	通过访谈安全主管，检查系统定级相关文档等过程，测评是否按照一定要求确定系统的安全等级。
2	安全方案设计	通过访谈系统建设负责人，检查系统安全建设方案等文档，测评系统整体的安全规划设计是否按照一定流程进行。
3	产品采购和使用	通过访谈安全主管、系统建设负责人和安全产品等过程，测评是否按照一定的要求进行系统的产品采购。

4	自行软件开发	通过访谈系统建设负责人，检查相关软件开发文档等，测评自行开发的软件是否采取必要的措施保证开发过程的安全性。
5	外包软件开发	通过访谈系统建设负责人，检查相关文档，测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。
6	工程实施	通过访谈系统建设负责人，检查相关文档，测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。
7	测试验收	通过访谈系统建设负责人，检查测试验收等相关文档，测评系统运行前是否对其进行测试验收工作。
8	系统交付	通过访谈系统运维负责人，检查系统交付清单等过程，测评是否采取必要的措施对系统交付过程进行有效控制。
9	等级测评	通过访谈系统运维负责人，核查定期开展等级测评和等级保护整改情况。
10	服务供应商选择	通过访谈系统运维负责人，测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

10. 安全运维管理测评

安全运维管理测评将通过访谈和检查的形式评测系统运维管理过程中的安全控制情况。主要涉及安全主管人员、安全管理人员、各类运维人员、各类管理制度、操作规程文件、执行过程记录等对象。

在内容上，系统运维管理测评实施过程涉及14个工作单元，具体如下表:

序号	安全子类	测评指标描述
1	环境管理	通过访谈物理安全负责人，检查机房安全管理制度，机房和办公环境等过程，测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。
2	资产管理	通过访谈资产管理员，检查资产清单，检查系统、网络设备等过程，测评是否采取必要的措施对系统的资产进行分类标识管理。
3	介质管理	通过访谈资产管理员，检查介质管理记录和各类介质等过程，测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。
4	设备维护管理	通过访谈资产管理员、系统管理员，检查设备使用管理文档和设备操作规程等过程，测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。
5	漏洞和风险管理	通过访谈安全主管、系统管理员，检查系统安全管理制度、系统审计日志和系统漏洞扫描报告等过程，测

		评是否采取必要的措施对系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。
6	网络和系统安全管理	通过访谈安全主管、网络管理员，检查网络安全管理制度、网络审计日志和网络漏洞扫描报告等过程，测评是否采取必要的措施对网络的安全配置、网络用户权限和审计日志等方面进行有效的管理，确保网络安全运行。
7	恶意代码防范管理	通过访谈系统运维负责人，检查恶意代码防范管理文档和恶意代码检测记录等过程，测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。
8	配置管理	通过访谈系统运维负责人，核查配置库的建立和维护情况。
9	密码管理	通过访谈安全员，测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。
10	变更管理	通过访谈系统运维负责人，检查变更方案和变更管理制度等过程，测评是否采取必要的措施对系统发生的变更进行有效管理。
11	备份与恢复管理	通过访谈系统管理员、网络管理员，检查系统备份管理文档和记录等过程，测评是否采取必要的措施对重

		要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。
12	安全事件处置	通过访谈系统运维负责人，检查安全事件记录分析文档、安全事件报告和处置管理制度等过程，测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。
13	应急预案管理	通过访谈系统运维负责人，检查应急响应预案文档等过程，测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。
14	外部运维管理	通过访谈系统运维负责人，核查外包运维服务商选择和安全相关协议的签订情况。

11. 工具测试

根据工具测试过程管理表单，使用漏洞扫描工具对信息系统的设备进行扫描，扫描结束后，根据目标设备的具体情况，判断漏洞验证的风险程度。

（五）实施流程

1. 测评准备活动：测评准备活动中，投标人主要完成启动测评项目，组建测评项目组；通过收集和分析被测系统的相关资料信息，掌握被测系统的大体情况；并准备测评工具和表单等测评所需的相关资料。

2. 方案编制活动：方案编制活动中，投标人主要完成确定测评对象和测评指标，选择测试工具接入点，从而进一步确定测评实施内容，并从已有的测评指导书中选择本次需要用到的测评指导书，最后根据上述情况编制测评方案。

3. 现场测评活动：现场测评活动中，投标人在与测评委托单位就测评方案达成一致意见，并进一步确定测评配合人员，完成测评指导书各项测评内容，获取足够的测评证据。

4. 分析与报告编制活动：分析与报告编制活动中，测评人员通过分析现场测评获得的测评证据和资料，判定单项测评结果及单元测评结果，进行整体测评和风险分析，形成等级测评结论，并编制测评报告。

（六）技术服务要求

1. 本次等级测评应满足的原则

投标人应严格依据下列原则和国家等级保护相关标准开展项目实施工作。

（1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标人的行为，否则招标人有权追究投标人的责任。

（2）标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

（3）规范性原则：投标人的工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

（4）可控性原则：测评服务的进度要跟上进度表的安排，保证

招标人对于测评工作的可控性。

（5）整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

（6）最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的的正常运行、业务的正常开展产生任何影响。

2. 本次等级测评的整体要求

（1）投标人应详细描述本次信息系统安全等级保护测评的整体实施方案，包括项目概述、等级保护测评方案、测试过程中需使用测试设备清单、时间安排、阶段性文档提交等。

（2）投标人应详细描述测评人员的组成、资质及各自职责的划分。投标人应配置有测评资质的专业人员进行本次信息安全等级保护测评工作。

（3）本次信息系统安全等级保护测评实施过程中所使用到的各种工具软件由投标人推荐，经招标人确认后由投标人提供并在信息系统等级保护测评中使用。

（4）信息系统安全等级保护测评需要的运行环境（如场地、网络环境等）由招标人提供，投标人应详细描述需要的运行环境的具体要求。

七、具体服务内容

序号	服务名称	服务内容	数量	备注
1	等保测评	定级备案	1 次	按照等保 2.0 三级要求对系统进

		专家评审	1 次	行测评。
		差距分析	1 次	
		等保测评	1 次	

八、检测时间要求

项目时间要求合同生效之日起，项目整体建设完成并验收合格时止。

九、交付成果要求

交付成果需满足长沙市数据资源管理局关于信息化项目的验收标准。

十、其他相关要求及说明

1. 服务地点：长沙市公安局交通警察支队。

2. 长沙市智能交通管理系统（第三期续建）项目竣工验收后，视长沙市智能交通管理系统（第三期续建）项目专项经费拨款情况一次性支付 100%。

3. 本项目采用费用包干方式，中标方应根据长沙市智能交通管理系统（第三期续建）项目的设计文件、招标文件以及合同内容完成测评工作，确保长沙市智能交通管理系统（第三期续建）项目在等保测评方面达到竣工验收要求，一旦成交，在本项目实施中出现任何遗漏，均由中标方免费提供，我单位不再支付任何费用。