**海曙智能防控平台审计系统**

# 项目背景

随着公安信息化向“大整合、高共享、深应用”快速发展，公安信息资源种类和数据激增，信息集中度和敏感度明显增加，信息应用和共享方式日趋复杂，数据盗取、越权访问等造成公安敏感信息泄露、侵犯公民隐私的现象时有发生，严重威胁公安信息网安全，亟待从安全技术手段上加强对公安信息资源的保护。海曙智能防控平台上线应用已有一段时间，针对平台在本局越来越频繁使用的情况下，为切实加强保密教育和管理，严格遵守各项法律法规和警务工作规定，坚决杜绝违规查询、泄露信息等违反“公安信息共享查询应用七不准”的行为,建设海曙智能防控平台审计系统。

# 建设目标

建设并部署日志审计系统，实现对海曙智能防控平台中各模块的日志信息的集中采集、预警监测和处置管理，为授权管理、取证核查、协查办案提供信息化辅助手段。

按《公安信息系统应用日志安全审计平台日志采集规范》标准格式采集和存储日志，实现数据查询、统计和分析。

建立与平台相配套的运维管理工作机制，构建起与公安信息化建设应用模式相适应的公安信息系统应用安全审计工作体系。

# 建设内容

## 日志采集存储

对海曙智能防控平台各模块的访问及操作行为的日志信息进行监测、采集及存储，以备倒查追踪。采集内容包括平台综合应用界面中涉及的关于反恐类、治安类、即时处置类、禁毒类、刑侦类、情指类、工具类等各模块，内容涵盖详情查看、更多列表查看、检索操作等。模块数量不少于125个，具体如下：

|  |  |
| --- | --- |
| **序号** | **功能名称** |
| 1. | 在逃人员预警处置 |
| 2. | 临控人员预警处置 |
| 3. | 涉毒脱失预警处置 |
| 4. | 涉毒逃避检测预警处置 |
| 5. | 涉稳即时预警 |
| 6. | 涉疆即时预警 |
| 7. | 外来涉疆预警 |
| 8. | 涉毒即时预警 |
| 9. | 涉黄即时预警 |
| 10. | 涉赌即时预警 |
| 11. | 扒窃周积分预警 |
| 12. | 扒窃月积分预警 |
| 13. | 扒窃即时预警 |
| 14. | 小区智清 |
| 15. | 小区基本信息 |
| 16. | 建筑物立体展示 |
| 17. | 有身份未登记预警 |
| 18. | 无身份未登记预警 |
| 19. | 有身份未登记关注人员 |
| 20. | 疑似离开预警 |
| 21. | 事件全息档案 |
| 22. | 作战图 |
| 23. | 领导批示 |
| 24. | 最新消息 |
| 25. | 指令反馈 |
| 26. | 重点人员 |
| 27. | 方案预案-法制保障 |
| 28. | 综合协调组 |
| 29. | 情报信息研判组 |
| 30. | 重点部位感知 |
| 31. | 网上信息查控组 |
| 32. | 重点对象侦控组 |
| 33. | 派出所组 |
| 34. | 落地谈话训诫组 |
| 35. | 重点人员人像感知 |
| 36. | 重点人员车辆感知 |
| 37. | 重点人员MAC感知 |
| 38. | 重点人员RFID感知 |
| 39. | 其他组信息汇总 |
| 40. | 微信群信息 |
| 41. | 宣传奖励 |
| 42. | 警情清零信息 |
| 43. | 未清零数据显示 |
| 44. | 可防控类别分析 |
| 45. | 黄赌毒举报社区排行 |
| 46. | 辖区宏观分析 |
| 47. | 辖区分项宏观分析 |
| 48. | 辖区子项宏观分析 |
| 49. | 社会治安类社区排名 |
| 50. | 宏观警情分析 |
| 51. | 警情分项分析 |
| 52. | 警情子项分析 |
| 53. | 多次报警分析 |
| 54. | 涉毒即时预警(区域) |
| 55. | 涉毒人员聚集预警 |
| 56. | 到站涉毒人员预警 |
| 57. | 同车次同旅馆涉毒人员预警 |
| 58. | 来甬疑似未登记 |
| 59. | 来甬公复场所预警 |
| 60. | 校门卫士-即时预警 |
| 61. | 校门卫士-长时间逗留 |
| 62. | 涉毒人员即时预警 |
| 63. | 隐性吸毒人员预警 |
| 64. | 射频感知预警 |
| 65. | 涉疆射频即时预警 |
| 66. | 被盗电动车登记 |
| 67. | 被盗电动车预警 |
| 68. | 涉疆聚集预警 |
| 69. | 涉稳聚集预警 |
| 70. | 涉赌聚集预警 |
| 71. | 涉赌积分预警 |
| 72. | 疑似毒驾预警 |
| 73. | 隐性吸毒聚集预警 |
| 74. | MAC涉毒聚集预警 |
| 75. | 毒驾人车计算 |
| 76. | 前科聚集预警 |
| 77. | 暂住人口住址变更 |
| 78. | 旅馆地区预警 |
| 79. | 维稳安保 |
| 80. | 涉毒关系网 |
| 81. | 视频设备规划图 |
| 82. | 设备分布情况 |
| 83. | 设备分布图 |
| 84. | 设备归属情况 |
| 85. | 长期入住旅馆预警 |
| 86. | 长期在住旅馆预警 |
| 87. | 旅馆同时登记预警 |
| 88. | 旅馆前科未登记 |
| 89. | 旅馆涉毒未登记 |
| 90. | 旅馆涉疆未登记 |
| 91. | 旅馆涉黄未登记 |
| 92. | 娱乐从业人员即时预警 |
| 93. | 娱乐从业人员聚集预警 |
| 94. | 娱乐从业人员积分预警 |
| 95. | 散装汽油多次预警 |
| 96. | 汽油关联警情预警 |
| 97. | 散装汽油登记预警 |
| 98. | 涉稳加油登记预警 |
| 99. | 涉疆加油登记预警 |
| 100. | 立案同比分析 |
| 101. | 立案均值分析 |
| 102. | 立案分析预警 |
| 103. | 警情 |
| 104. | 接警同比分析 |
| 105. | 接警均值分析 |
| 106. | 接警分析预警 |
| 107. | 处警时效分析 |
| 108. | 秘拍人员预警 |
| 109. | 秘拍人员积分 |
| 110. | 在逃人员线索信息登记 |
| 111. | 应急处置 |
| 112. | 一图展示 |
| 113. | 由人到案 |
| 114. | 由案到人 |
| 115. | 人员关系研判 |
| 116. | 人像单一检索 |
| 117. | 人像单一检索（设备） |
| 118. | MAC单一检索 |
| 119. | RFID单一检索 |
| 120. | 海曙车辆全量数据检索 |
| 121. | MAC碰撞计算 |
| 122. | RFID碰撞计算 |
| 123. | 车辆碰撞计算 |
| 124. | 关系人检索 |
| 125. | 警务通GPS检索 |

采集存储信息要求包括用户标识、单位名称、用户名、终端标识、操作类型、操作时间、操作条件、操作结果等，且日志存储支持一年在线数据查询。

## 日志查询统计

可对一定时间内的日志记录进行查询统计分析，包括各类操作人员、操作次数、操作频率等，支持根据模块、操作类型、操作人员、操作部门、操作时间等进行查询。

系统每日自动进行统计，统计人员日、周、月、总的登录数量、访问数量及检索数量。

## 日志可视化展示

结合图表等各类可视化工具显示系统整体访问情况。

分析民警集中访问时段，显示访问人数、次数等。

显示模块访问排行，分析民警日常关注及受欢迎的模块,可作为平台日后优化完善的依据，对民警关注的模块进一步推广落地，对民警不关注的模块可进行去除或改进。

支持根据人员或部门统计访问排行情况。

**本次采购最高限价276500元。**