第三章　招标需求

序号	事 项	内 容
1	采购单位	上海市公安局黄浦分局（本级）
2	项目名称	**上海市公安局黄浦分局（本级）——数据安全平台采购项目**
3	采购预算金额	2,130,000.00 元（国库资金：2,130,000.00 元）
4	项目属性	服务类
5	采购意向是否已公开	已于 2024 年 11 月 1 日发布意向公开公告
6	采购标的所属行业 **（按工信部联企业〔2011〕300 号文件内容划分，仅用于中小微企业认定）**	软件和信息技术服务业
7	特定资格要求	无
8	是否专门面向中小微企业	**否**
9	是否招一用三	否
10	合同履行期限【建设周期】	合同签订后 45 日历天
11	质保或免费维护期	项目验收通过后不少于三年
12	是否允许联合体投标	否
13	是否允许采购进口产品	否
14	是否现场踏勘	否
15	付款方式	**(1) 合同签订项目启动后支付 30%** **(2) 系统平台上线运行 50%** (3) **试运行一个月且通过验收后 20%**
16	验收方式	采购人自行组织验收考核
17	本项目询问、质疑受理委托授权范围	采购人授权采购中心受理和答复本项目潜在投标人依法提出的询问和质疑
18	本项目是否属于政务信息系统（信息化项目填写）	否
19	本项目评审办法	综合评分法

一、项目招标范围及内容

1.采购目标

通过采购数据安全平台相关硬件和软件，实时掌握上海市公安黄浦分局数据安全态势，全量数据资产和风险隐患，提升数据交互场景下的监测预警能力，落实数据安全职责，形成数据安全全生命周期的管理体系，最终实现上海公安数据安全“两级联动、闭环处置”的目标。

2.采购范围

本次采购范围为黄浦分局新一代公安信息网内数据安全监测及数据安全加固等软硬件设备。

3.采购内容

本次项目重点采购 1 套平台（硬件设备+成品软件）和 3 类探针（软硬一体设备）。其中 1 套平台指的是数据安全平台硬件及软件；3 类探针分别为数据扫描探针、API 风险发现探针、数据流转探针；平台需提供北向接口，与市局平台进行对接，对数据资产、安全评估、风险预警等信息进行上报。

4.招标内容与指标要求

4.1 采购硬件清单

序号	产品名称	数量	备注
1	数据安全平台	3 台	专用硬件
2	API 风险发现探针	1 台	软硬一体
3	数据流转探针	1 台	软硬一体
4	数据扫描探针	1 台	软硬一体

4.2 采购软件清单

序号	产品名称	产品能力	数量	备注
1	数据安全平台软件	包含数据安全资产梳理功能、数据安全风险发现功能、指定类型数据识别、数据安全态势运营功能、日志统一管理功能、流转链路测绘功能、业务数据建模功能，具备公安网内数据资产风险事件的实时发现能力，达到以网络访问、API、应用系统、数据库等多层次的资产全方位安全视角，聚焦实时构建数据资产全生命周期内外部流转链路，为数据安全风险发现和管控提供可视化支撑。对特定数据的全网数据流转拓扑自动梳理。达到以全局的业务视角发现应用，数据库，API，账号，人员等所产生的数据安全风险，并进行有效的数据安全管控和可视化支撑。	1 套	

★ 除采购需求另有明确约定以外，本项目投标产品涉及台式计算机、便携式计算机、一体式计算机、工作站、通用服务器、操作系统、数据库等七类信息化产品的，必须符合现行《政府采购需求标准》（财政部、工业和信息化部所制定）的强制性规定；所投产品的 CPU、操作系统必须符合安全可靠测评要求，同时所投产品必须满足《政府采购需求标准》内的所有强制性要求。（投标人须按照本项目招标文件第三章 招标需求“ 附件：★承诺函格式”提供承诺）

4.3 具体技术指标要求

4.3.1 数据安全平台（硬件）

2U 设备；CPU≥24 核；内存≥256G；硬盘≥36T；接口≥4 个千兆电，国产操作系统。

4.3.2 API 风险发现探针要求

1)2U 设备；CPU≥24 核；内存≥64G；硬盘≥20TB；接口≥4 个千兆电，2 个万兆光口；冗余电源，流量接收峰值≥5Gbps 国产操作系统；

2)需支持以 agent 和镜像流量混合模式采集流量，支持以源 IP 或 IP 段、目的 IP 或 IP 段、域名、URL 通配符、请求头、响应头、响应码、请求方法、域名等指标组合配置分析流量或过滤流量数据；

3)需支持自动识别公安网流量中的应用系统，形成应用清单；支持列表结构呈现 API 清单，包括 API 基本信息：名称、路径、类型、访问量、访问域、部署域、发现时间、活跃时间等；支持列表结构呈现账号清单，展示相关的基本信息：生命周期、发现时间、活跃时间；支持展示账号关联信息：应用名称、应用状态、组织架构；

4)自动识别公安网内文件中包含的指定类型数据标签。支持识别文件类型包括：doc、pdf、docx、xls、xlsx、ppt、zip、rar、tar、gz、7z、docm、pptm、xltm、xlsb、bz2、gzip、wps、txt、html、xml、csv、json等；

5)支持在公安网内根据策略自动识别划分静态资源页面和数据共享API，支持可视化多指标组合配置划分规则，配置指标维度包括：URL、请求用户代理、请求方法、响应内容类型、请求头、响应头、响应码、请求体、响应体；

6)支持在公安网内以IP、账号、IP+API、账号+API、数据维度进行行为风险配置。支持通过多种指标组合自定义配置新增风险策略，例如：请求数据标签、返回数据标签、下载文件、上传文件、访问频次、登录数、验证码去重数、操作时间等。支持以滑动窗口计数方式匹配监测规则；

7)支持在公安网内根据指定类型数据进行数据溯源。可通过发生时间、应用名称、API、账号、客户端IP、分析ID、会话ID、文件名称、响应关键字、请求关键字、请求数据标签、返回数据标签等条件进行溯源结果的筛选；

8)API风险发现探针从架构上是为平台软件提供数据的采集工作，探针需与平台软件的数据完成适配；

9)**按照相关国家标准的强制性要求，由具备资格的机构出具的安全认证合格或者安全检测符合的认证证书。**

4.3.3 数据流转探针要求

1)2U设备；CPU≥24核；内存≥64G；数据盘≥20TB；冗余电源；接口≥4个千兆电，2个万兆光口；流量接收峰值≥10Gbps；国产操作系统；

2)支持主流数据库及国产化数据库的分析能力，包括但不限于下列数据库：支持Oracle（包括21C及其他版本）、ClickHouse、Cache（包括2021及其他版本）、PostgreSQL（14及其他版本）、MySQL、SQL Server、Sybase、DB2、Informix、Graphbase、ArangoDB等；包含但不限于下列国产数据库：达梦、南大通用(GBase)、高斯（GaussDB）、人大金仓（KingbaseV8、V7及其他版本）、神舟通用（Oscar）、OceanBase、瀚高（HighGo DB)等；

3)支持HDFS、HIVE、PostgreSQL等场景下的kerberos认证加密流量的解析与记录；

4)分析能力能够支持记录执行时长、影响行数、执行结果描述、返回结果集；

5)支持本地直连数据库场景下的分析，实现对本地运维人员的数据库操作行为的分析，支持主流数据库如Oracle、PostgreSQL、MySQL、SQL Server等；

6)为配合风险溯源能力，需支持日志查询时分析筛选能力，根据查询条件自动分析出存在的数据库账号、客户端IP、客户端工具、操作系统用户名、服务端IP、操作类型、数据库名/实例名、表名、主机名、执行状态、执行时长、影响行数等；

7)数据流转探针从架构上是为平台软件提供数据的采集工作，探针需与平台软件的数据完成适配；

8)**按照相关国家标准的强制性要求，由具备资格的机构出具的安全认证合格或者安全检测符合的认证证书。**

4.3.4 数据扫描探针要求

1)2U 设备；CPU≥24 核；内存≥32G；数据盘≥8T；冗余电源；接口≥5 个千兆电口，国产操作系统；

2)支持主流数据库及国产化数据库的扫描能力，包括但不限于下列数据库：支持 Oracle、ClickHouse、Cache、PostgreSQL、MySQL、SQL Server、Sybase、DB2、Informix 等数据库类型，包含但不限于下列国产数据库：达梦、南大通用(GBase)、高斯（GaussDB)、人大金仓（KingbaseV8、V7 及其他版本)、神舟通用（Oscar)、OceanBase 等；

3)支持对于已经创建的数据源上传其对应的数据字典信息，以对于表注释及字段注释进行补充；

4)支持对于数据源中所包含的数据质量进行评估，评估指标包含：字段总数、字段注释存在数、有含义的字段注释数、有含义的字段注释去重数、表总数、表注释存在数、有含义的表注释数、有含义的表注释去重数；

5)支持通过联动数据流转探针设备，解析被记录语句中的数据库资产信息，实现数据库资产的被动发现；

6)支持对于非结构化文件进行分类分级，可支持的文件类型包括：docx/doc/txt/pdf/dcm，且可指定非结构化行业模版，以及支持行业模版的维护；

7)数据扫描探针从架构上是为平台软件提供数据的采集工作，探针需与平台软件的数据完成适配；

8)**按照相关国家标准的强制性要求，由具备资格的机构出具的安全认证合格或者安全检测符合的认证证书。**

4.3.5 数据安全平台软件（成品软件）

包含公安网内数据资产梳理功能、数据安全风险感知功能、指定类型数据识别、数据安全态势运营功能、日志统一管理功能、流转链路测绘功能、业务数据建模功能，具备数据资产风险事件的实时监测能力，达到以网络访问、API、应用系统、数据库等多层次的资产全方位安全视角，聚焦实时构建数据资产全生命周期内流转链路，为数据安全风险感知和管控提供可视化支撑。对特定数据的数据流转拓扑自动梳理。达到以全局的业务视角感知应用，数据库，API，账号等所产生的数据安全风险，并进行有效的数据安全管控和可视化支撑。具体功能要求如下：

1)提供公安网内数据安全运营所需的数据、策略、监控、事件等的可视化展示。对资产底账排查、安全风险事件处置、日常流量监测、防护能力覆盖等平台的日常运营情况进行可视化呈现；

2)应支持将公安网内数据资产按照数据库、数据表、数据字段的结构进行管理。支持数据库自动发现、人工录入、批量导入并提供 excel 导入模版、导出、查看档案详情、新增、查询、删除等功能，将用户的数

据库进行统一管理，建立全局的数据资源目录；

3)应支持按梳理过的数据库数量、指定类型数据库数量、数据表数量、指定类型数据表数量、数据字段数量、指定类型数据字段数量，数据表和数据列的安全级别分布进行统计；

4)统计展示指定类型数据占比以及数据分类分级的完成度；

5)支持查看事件详情信息，包括但不限于：事件类型、事件等级、事件验证情况、单位名称、事件名称、发现时间、来源 IP、目的 IP 等；安全事件详情支持追踪溯源至原始告警；

6)支持告警聚合自动化匹配规则模型生成安全事件， 并支持自定义配置规则模型、聚合时间、聚合字段；

7)工单详情支持显示多类工单相关信息，包括但不限于工单标题、工单标签、所属单位、发起单位、工单完整流程及当前所处流程、工单正文、处理记录等；

8)支持工单流程可配置、支持对工单内容配置、满足工单系统级联对接；

9)需提供公安网内数据上报功能，保障本级单位安全运营数据能有效上报至上级单位。

二、售后服务要求

1.硬件部分要求

1.1 项目实施中，对于有质量异议的设备、材料、构配件等物料，不符合招标要求的，中标人需无条件将不符合招标要求的产品设备更换为满足招标要求的产品设备；

1.2 项目采购和验收过程中，若发现相关内容未达到招标需求的目标、任务和要求，中标人需自行改进，直至达到招标需求的目标、任务和要求，所产生的额外费用由中标人承担；

1.3 对于满足招标需求的中标产品，中标人不得以任何借口，改变中标产品的品牌型号或减少中标产品数量；

1.4 中标人应在合同规定的时间内按采购人要求完成硬件部署、调试、验收工作。

2.软件部分要求

2.1 项目实施中，中标人存在不符合招标要求的情况，中标人需无条件修改或重新开发，直至满足招标要求，所产生的额外费用由中标人承担；

2.2 中标人需保证所配置的软件产品有合法的使用权；

2.3 中标人应在合同规定的时间内按采购人要求完成软件部署、调试、验收工作；

2.4 中标人就应用软件操作、维护，对用户方的相关技术人员和使用人员进行现场技术培训，达到正确使用与维护的水平。采购人受训人员的培训费用由中标人承担；

2.5 中标人应就软件提供完整的安装调试、系统配置、操作说明等相关技术文档。

3.运维服务要求

3.1 本项目需满足与上级单位的数据对接。本项目涉及软件部分需确保系统间数据的顺畅传输与硬件的稳定运行。按照上海市相关采购指导意见及目标，进行系统架构的设计，确保完成上海市公安“两级联动，闭环处置”的总体目标。具体要求如下：

3.2 与上级单位的数据对接由本项目负责实施；

3.3 中标人的项目建设需通过上级单位的评估验收，如未达到验收标准，中标人需无条件修改或重新开发，直至满足验收要求；

3.4 中标人按照服务质量标准提供各种售后服务；

3.5 在中标人服务期内，负责本项目的维护工作，确保系统安全、稳定、正常地运行并对由于设计、功能的缺陷而产生的故障负责。中标人提供 7 天×24 小时的运维服务保障。在此期间如发生系统运作故障，或出现瑕疵，中标人将按照售后服务的承诺提供保修和维护服务。中标人提供多种技术支持方式：

（1）远程支持：中标人需提供指定服务电话，对使用本项目涉及的软硬件和服务遇到的各种问题和困难，提供 7 天×24 小时问题咨询及远程安全技术支持服务；

（2）现场支持：无法通过在线方式解决问题，必须现场处理，中标人需派遣工程师赶赴现场分析故障原因，制定故障排除方案，提供故障排除服务。遇到重大故障，现场人员 12 小时内无法解决的应在 24 小时内提供不低于故障设备性能的备件。产品由于非不可抗力导致设备故障、无法运行的，相关设备更换及软件更换费用由中标人支付。

4.日常维护方案。投标人提供的方案里需包含售后服务内容、故障响应时间、售后技术支持内容、风险分析及处理方法。

三、拟提供项目人员要求：开发过程中在公安机关驻场办公，运维期间保持 24 小时电话畅通，系统发生故障后立即协助开展处置工作，无法远程处置的需 1 小时内到现场开展处置工作。

四、付款及验收要求：

1.付款要求：

(1)合同签订项目启动后支付 30%

(2)系统平台上线运行 50%

(3) 试运行一个月且通过验收后20%

2．验收要求：

（一）建设运维

（1）建设要求

①按要求部署“一平台，三探针”且性能符合市局标准。

②流量采集覆盖全分局各单位。

（2）安全管理

具备平台操作安全，异常账号的锁定及强制下线能力等安全措施。

（二）主要功能

（1）资产台账建设

①数据资产台账能力建设，能实时识别资产变化，数据资产类型至少包含应用、数据库、人员账号、API 接口、文件，组织架构和网络资产。

②将资产台账数据按要求同步至市局，并在数据资产中包含数据量及数据更新时间信息，同时上报的数据资产均需在市局数据资产管理系统中进行编目。

③对扫描探针及流量探针识别的分局各单位数据库和数据资源进行全量纳管并上报至市局平台。

（2）敏感识别建设

按照市局敏感关键字标准完成数据敏感识别及梳理工作，并通过市局系统校验。

（3）分类分级建设

完成数据分类分级能力建设，对分局数据资产进行分类分级，并通过市局系统校验。

（三）风险监测建设

1.完成数据安全风险的自动感知能力建设，并可通过可视化技术展示风险详情，至少包含（风险类型、风险等级、风险验证情况、单位名称、风险名称、资产名称、风险开始时间、风险结束时间、原始告警等）。

2.利用数据安全风险监测功能开展分局风险处置工作，并通过市局系统校验。

（四）安全运营建设

1． 完成分局内部风险、事件的流程处置能力建设，可通过工单形式进行安全事件的闭环研判处置。

2.可通过多种视角展示数据安全风险，监理资产网络拓扑、业务属性、数据资产、资产所有者、数据使用方等多维度间关系，完成数据安全整体运营能力。

3.可顺利接受市局下发的任务工单，并完成反馈。

五、数据管理

（1）策略接收

完成与市局平台的数据对接能力，可接收市局平台下发的安全策略，并执行反馈。

（2）数据建模

1．在平台内完成分局自身数据安全建模能力建设，并可根据业务场景自定义模型。

2.完成一个分局数据安全风险特色模型的建设、并通过市局系统校验。

（3）日志上报

1．完成数据库操作日志的全量上报，配合开展日志统一汇聚任务，并通过市局系统校验。

2.完成网络流量的全量上报，配合开展日志统一汇聚任务，并通过市局系统校验。

六、其他要求：

1.关于转让和分包的规定

本项目不得转让、不得分包。

2.知识产权及保密要求

(1)中标人数据、文件、资料知识产权

中标人保证其所提供的服务和交付的成果以及在履行本项目义务中使用到的所有数据、文件、信息不会引起任何第三方在专利权、著作权、商标权等知识产权方面向采购人或采购人的关联方及合作方（包括但不限于采购人的主管单位和采购人的合作单位等）发出侵权指控或提出索赔。若有，中标人应负责与第三方解决纠纷，若因此导致采购人损失的，采购人有权要求中标人赔偿采购人因此遭受的全部损失，包括但不限于直接损失、间接损失、诉讼费／仲裁费、律师费、公证费、鉴定费等。

中标人因履行本项目而产生的所有成果的知识产权等权利均归采购人所有，中标人应配合采购人进行相关权利登记或申请。未经采购人书面同意，中标人不得以任何形式使用或许可他人使用本项目成果的相关内容，不得擅自对外公开发表或向任何第三方透露。

在不影响上述条款规定的由采购人取得所有成果的知识产权的前提下，双方因履行本项目而被授权接触或使用对方之知识产权（包括但不限于商标、专利、著作权等），和/或任何其他相关资料、数据等涉及的任何权利，均不视为向另一方转让上述权利或在本项目范围外授权许可另一方使用上述权利，上述权利仍应属于提供方，并仅可使用于本项目，被授权接触或使用方未经提供方书面同意，不得擅自挪作他用。

(2)项目保密要求

中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，中标人不得对外泄露采购人要求保密的信息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及中标人的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标人人员或中标人合作方违反保密规定，中标人应承担连带责任。

中标人（含中标人参与本项目的人员以及其合作方）未经采购方书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、

技术诀窍、秘密信息、技术资料和其他文件。

以上内容的保密期限自中标人知悉保密信息起始至保密信息被合法公开之日止。

(3)临时账号等使用要求

中标人对采购人提拱的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息安全的泄露。未经采购人的同意不得利用采购人的网络及平台进行短信、彩信、微信发送,造成的一切后果由中标人负责。

七、“★”号“＃”号汇总

★重要提示：投标人必须对本技术规格要求逐条响应“★”号为必须实质响应的内容，若无法满足，作无效标处理；“#”号为主要指标，未提供或提供不完整的，均不得分。

为提高评审效率方便评委核查，招标文件凡涉及以下“★”号指标和“＃”号指标要求的响应情况及内容应当按照“第六章投标文件格式参考，表格 1、招标需求索引表”的格式及要求制作索引表，不制作索引表或未按照要求逐一明确标注相关内容所在页码的，可能导致评委会无法准确查找到相关重要响应内容，由此产生的不利后果由投标人自行承担。

“★”号指标汇总表：

序号	名称	技术指标
1	资格性审查要求（由采购人审核）	（1）**营业执照：** 投标人应提供营业执照（或事业单位、社会团体法人证书）的**清晰扫描件**。 **投标人未按照要求提供的，作无效标处理。** （2）**资格声明函：** 投标人须按招标文件“**第六章 投标文件参考格式，样式 3、资格声明函**”的格式填写，**必须包括该样式中所含的全部内容，并按其要求加盖投标人公章。** **投标人未提供或不按招标文件要求制作、签署的，作无效标处理。** （3）**法人代表授权书：** 投标人提供的法人代表授权书必须按本项目招标文件“**第六章 投标文件参考格式，样式4、法人代表授权书**”格式制作，且必须经单位负责人签字或盖章、 被授权人签字或盖章、加盖供应商单位公章；授权书中必须附带单位负责人和被授权人身份证的清晰扫描件。 **投标人未提供或不按招标文件要求制作、签署的，作无效标处理。**

		注：单位负责人是指单位法定代表人或者法律、行政法规规定代表单位行使职权的主要负责人。 **（4）信用记录查询：** **凡列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，其响应无效。** **注：投标人无需提供资料，由采购人或采购人授权的集中采购机构于开标后、评标前，通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别。**
2	**符合性审查要求**	**(1) ★承诺函：** **投标人须按照本项目招标文件“第三章 招标需求 附件：★承诺函格式”提供承诺函。** **投标人未按格式要求提供本承诺函、未提供此承诺函或未按要求签署盖章的,均作无效标处理。** **(2)法律、法规和招标文件规定的无效情形：** 包括但不限于：投标报价超财政预算或最高限价的；投标文件含有采购人不能接受的附加条件的；投标人存在串标、围标或以虚假材料谋取中标情形的；投标人报价明显过低，可能影响产品质量或诚信履约且无法证明报价合理性的；违反劳动法律法规，其他违法违规或违反招标文件约定构成无效标的情形。

本项目无#号指标

附件： **★承诺函格式**

★承诺函

（未按格式要求提供本承诺函、未提供此承诺函或未按要求签署盖章的,均作无效标处理）

致：上海市公安局黄浦分局（本级）

我司承诺：本项目投标产品涉及台式计算机、便携式计算机、一体式计算机、工作站、通用服务器、操作系统、数据库等七类信息化产品的，均符合现行《政府采购需求标准》（财政部、工业和信息化部所制定）的强制性规定；所投产品的 CPU、操作系统均符合安全可靠测评要求，同时所投产品均满足《政府采购需求标准》内的所有强制性要求。

本公司承诺完全响应以上要求，特此声明。

投标人授权代表签字：_____

投标人（公章）：

日期：_____年___月___日