A包采购需求

一、预算金额：人民币1064.81万元

二、系统软硬件采购列表

序号	类别		主要建设内容	数量	单位
1	信息触达宣防管理系统	公安网应用	详见“建设内容及技术要求”	1	套
2		政务外网应用	详见“建设内容及技术要求”	1	套
4		互联网应用	详见“建设内容及技术要求”	1	套
5		省通信管理局协同处置子系统	详见“建设内容及技术要求”	1	套
6	行业数据联动核查管控系统	系统应用功能	详见“建设内容及技术要求”	1	套
7		应用功能支撑管理	详见“建设内容及技术要求”	1	套
8		可信数据支撑管理	详见“建设内容及技术要求”	1	套
9		系统运行支撑管理	详见“建设内容及技术要求”	1	套
10		多方业务平台接入服务	详见“建设内容及技术要求”	1	套
11		边缘计算终端	详见“建设内容及技术要求”	5	套
12	侦查协作实战应用系统	联动核查数据服务	详见“建设内容及技术要求”	1	套

13		多流数据研判	详见“建设内容及技术要求”	1	套
14		在线协同办公	详见“建设内容及技术要求”	1	套
15		线索在线上报	详见“建设内容及技术要求”	1	套
16		系统支撑管理	详见“建设内容及技术要求”	1	套

三、系统规格及技术要求

3.1 项目建设基本情况

以省公安厅大数据实战应平台、省社管平台等系统平台为依托，以相关部门警种业务系统为支撑，充分运用大数据、云计算、智能合约、可信身份、数据存证、隐私保护等先进技术，搭建服务全省打击治理电信网络诈骗犯罪的信息触达宣防管理系统、行业数据联动核查管控系统和侦查协作实战应用系统，全面整合省打击治理电信网络新型违法犯罪联席会议成员单位和相关行业以及公安机关各警种、各部门、各专业手段资源优势，围绕实时警情、案件和突出治安问题，特别是电信网络诈骗犯罪持续多发高发的问题，积极推进、整体协作、同步上案、信息互通、无缝对接，实现“共享+合成”，依托社管平台能力资源充分调动社区网格员的力量，使下沉的人力有效聚合，实现反诈预警宣防信息的快速触达，提高反诈宣防的覆盖面和触达率，提升反诈宣防工作效能。

3.2 建设内容及技术要求

3.2.1 信息触达宣防管理系统

3.2.1.1 系统总体需求

信息触达宣防管理系统分为三个网端的应用，包括公安网、政务外网、互联网，其中公安网承担了数据分析、任务发起、结果分析等工作；政务外网承担了任务的管理、任务分发以及数据安全交互的任务；互联网负责接收宣防任务，并将宣防反馈的结果推送到政务外网，由政务外网将反馈结果推送到公安网。

省反诈平台通过专线将需要处置的涉诈信息推送到海南通信管理局协同处置子系统，对于省内可处置的电话及域名等，协同处置子系统与省运营商电话反诈系统及 DNS 系统等进行对接，形成自动化处置，运营商处置完成后，反馈处置信息至通信管理局并通过协同处置子系统转发至反诈中心。对于需要工信部反诈大平台进行处置的涉诈数据，协同处置子系统将涉诈数据上传工信部反诈大平台，待工信部处置完成后，反馈处置信息至省反诈平台。

3.2.1.2 系统功能模块需求

3.2.1.2.1 公安网应用

本侧应用建设在公安厅公安信息网，负责将我省潜在受害者结果数据通过安全边界传递至信息触达宣防管理系统，完成协同通管局和运营商开展技术阻断、分派处置潜在受害者劝阻、处理目标封堵举报投诉、工作成效评估及案件态势展示、诈涉重点人员管控等工作。

3.2.1.2.1.1 涉诈目标技术阻断

将涉诈相关信息第一时间送达三大运营商阻断、封停处置，并备案省通讯管理局，避免我省群众继续受骗。

1、公安侧发起

公安侧发出协同处置到通管局，通管局进行处置备案，并将处置任务发送到运营商，运营商接到处置任务后，快速完成处置，反馈结果推送到通管局报备。支持整个任务的状态跟踪和历史追溯。

2、运营商侧发起

运营商对自行发现的涉诈可疑信息做快速处置后，将处置的信息、处置的结果推送到通管局进行备案。通管局再推送到公安侧进行备案。

3、数据共享管理

公安侧发出涉案数据（非海南省）共享的请求到通管局，通管局进行共享备案后将共享的涉案数据对接到工信部，由工信部分发到各省的通管局以及互联网服务商进行处置，最大程度的拦截海南省民众访问外省涉案信息，减少海南省民众被骗的几率。

3.2.1.2.1.2 潜在受害者劝阻

接收“公安部反诈大数据平台”、“反诈预警综合分析系统”的推送的各类预警数据以及其第三方的预警数据，去重融合后、身份核验后推送到海南省打击电信网络诈骗犯罪合成作战平台，数据同步到96110电话平台、96110的短信发送平台以及智能AI机器人回访平台对预警数据进行劝阻，结果回填到海南省打击电信网络诈骗犯罪合成作战平台，系统劝阻回访工作进行统计分析。

对高危重点人群进行二次分级分类，对潜在受害者进行分级分类劝阻。

3.2.1.2.1.3 投诉信息处置

1、投诉处置

接警员接到投诉后，录入投诉的相关信息，通过数据核验对被处置账号的进行核验后选择投诉处置方式，包括解封、不予解封，并回复投诉者处置结果。

2、处置核查

系统定期核查错封和错解封的情况，将情况反馈到反诈中心，优化和调整预警模型和人员核查模型。

3、信息查询

支持多条件组合查询，通过列表的形式进行呈现，可设置特定的列进行排序，并支持查询结果的导出。

4、数据统计

支持多条件进行投诉信息的统计分析。以饼状、柱状、折线等形式宏观展现投诉的整体情况。

3.2.1.2.1.4 精准宣传任务下发

通过精准宣传提升我省公民的诈骗防范意识和降低场景、角色带来的诈骗可能性，来降低我省公民受骗率。

1、宣防任务数据分析

基于案件主题域数据、人员主题域数据、物品主题域数据，即人案物的综合分析，从案件数量、案件描述、人员特质等纵向、横向维度的分析，有针对性分析高发类型案件，并做及时推送预警。

潜在受害者分析模型：利用最新的预警数据和人员主题域数据、标签体系以及对应的案件主题域所关联的受害者属性、特征等维度分析，建立潜在受害者模型。

重点人群分析模型：分析案件中受害者的属性和特征，结合本辖区的人员结构特征，建立重点人群模型。

受害者关系分析模型：利用关系库、标签体系以及案件特征建立受害者关系分析模型，以便对受害人与之关联人群进行重点预警、宣传。

重点单位/机构分析模型：建立类案高发企业、机构分析模型，结合组织主题域数据，对组织机构进行特征分析。

最新犯罪手法分析模型：建立最新犯罪手法分析模型，对案件的特性进行深度分析，汇总各类违法犯罪的手法，对最新、高危等手法进行说明。

网格高危发案类型分析模型：结合组织主题域、地点主题域，并且结合宣防员提供的数据进行综合分析建模，对各个网格建立标签体系，人群特征值，分析出某区某社区某网格可能发生高危的案件类型。

发案趋势分析模型：通过历史案件数据进行大量数据的离散聚合分析，基于相关数据分析报告建立某地未来案件发案趋势分析模型。

异动人员分析模型：建立异动人员分析模型，及时发现异常轨迹，推送到前端，宣防员介入和干预后，及时将相关信息反馈到中心。

2、宣防任务下发

通过内外网安全交互平台将预警宣防数据推送到政务外网侧，为宣防员的宣防工作提供预警宣防数据、辖区人口数据以及辖区发案情况数据等。

3、基础支撑管理

设计系统接口，满足数据接收和推送的需求，适配数据库层面的对接和页面操作的对接等多种方式；系统提供接口监控的功能，实时监控接口运行的状态；可视化配置推送的内容、时间、周期，便于随着业务的调整动态适配宣防工作的要求；跟踪宣防任务的状态，便于及时掌握宣防任务的执行情况和执行效果。

3.2.1.2.1.5 涉诈重点人员管控

提取本地涉诈重点人员，获取涉诈重点人员的相关信息。

系统支持人员信息的批量导入，支持 Excel 导入及导入过程的数据校验，系统支持导入模板下载。

构建重点人行为预警模型，设置相关参数和权值。

利用数据接口，将涉诈重点人员信息推送管控负责人端，管控负责人可查看

重点人员的相关信息以及完成见面核查等。

支持多查询条件组合以及可设置根据特定的列对查询结果进行排序，并支持查询结果的导出保存。

通过多维度统计分析涉诈重点人员相关信息。以饼状、柱状、折线等形式宏观展现。

3.2.1.2.1.6 工作成效评估及案件态势展示

1、触达宣防工作分析

信息触达统计分析：多维度对宣防信息进行统计分析，及时展现宣防信息触达的总体情况，为反诈骗宣防工作提供决策依据。

触达情况与发案统计分析：依据网格反馈的信息触达情况和辖区发案的变化情况，对信息分析的相关模型及触达的时间进行评估，调整数据分析模型的维度、触达面以及时间。

辖区人员变化与案件趋势分析：结合流动人口信息和宣防员采集的流入人员信息，分析辖区内人员结构变化和发案趋势变化的关系。

涉诈重点人员管控分析：通过管控 APP 反馈的信息，综合分析涉诈重点人员管控情况，以可视化的形式展示分析结果。

2、接警信息分析

接警态势分析：可根据发案时间段、案件类型等条件进行发案趋势分析，以线形图进行直观展示。

按接警分类统计：根据时间段统计报警分类，将案件信息以多维度进行分别展示。

3、预警回访分析

派警情况统计分析：根据时间段统计辖区各地市派警情况，将派警数量进行统计分析，通过柱状图的形式进行展示。

疑号推送统计分析：提供疑号推送类数据统计分析，并可根据日、周、月、年度等时间维度进行统计展示。

高危交易统计分析：提供高危交易类数据统计分析，并可根据日、周、月、年度等时间维度进行统计展示。

APP 诈骗统计分析：提供 APP 诈骗类数据统计分析，并可根据日、周、月、

年度等时间维度进行统计展示。

人工劝阻统计分析：根据时间段统计辖区各地市人工劝阻情况，将人工劝阻数量进行统计展示。

上门劝阻统计分析：根据时间段统计辖区各地市上门劝阻情况，将上门劝阻数量进行统计展示。

AI 预警回访统分析:根据时间段统计辖区各地市智能 AI 语音预警回访情况，将智能 AI 语音预警回访数量进行统计展示。

预警线索上报统计分析：根据时间段统计辖区各地市预警线索数据上报情况，将线索上报数量进行统计展示。

4、受害人分析

受骗人性别分析:对受骗人的性别进行统计分析,并以饼状图进行直观展示。

受骗人年龄分析：对受骗人的年龄段进行统计分析，并以柱状图进行直观展示。

受骗地区分析：对受骗地区的发案数量进行统计分析，并以柱状图进行直观展示。

受骗人号码所属运营商分析：对受骗人的号码所属运营商进行统计分析，并以饼状图进行直观展示。

受骗人银行卡分析：对受骗人银行卡的所属银行、卡号名称、卡类型进行分析，统计其数量、占比等情况，支持以柱状图的形式展示排名靠前的信息。

5、嫌疑人分析

嫌疑人号码所属运营商分析：对嫌疑人的号码所属运营商进行统计分析，支持以饼状图进行直观展示。

嫌疑人银行卡分析：对嫌疑人的银行卡的所属银行、卡号名称、卡类型进行分析，统计其数量、占比等情况，支持以饼状图的形式展示。

6、案件特征分析

对诈骗案件所使用的主要通讯工具、引流渠道等维度分析我省电信网络诈骗犯罪的特征变化，指导涉诈灰黑产打击、整治方向和反诈预警综合分析系统模型设计重点。以饼状、柱状、折线等形式呈现 案件特征的分析结果，系统支持统计分析维度的调整，快速适应相关统计需求的变化。

7、警情大屏展示

提供警情数据的大屏展示功能，展示内容包含：警情统计（案件、举报、咨询）、涉案金额、最新警情信息、各市县警情情况占比、诈骗类型 TOP10 等。

8、预警大屏展示

提供预警数据的大屏展示功能，展示内容包含：劝阻金额统计、AI 回访记录、人工回访数量、AI 回访数量、最新上门回访情况、预警来源准确率统计、预警数据占比等。

3.2.1.2.1.7 系统管理

系统配置管理包括人员、角色、权限等添加、删除、修改等，以统一的入口实现对系统操作员的配置和管理。

参数配置管理包括数据字典管理、系统显示管理等。通过设置不同的参数配置实现系统的显示风格、字典维护的动态调整。

3.2.1.2.2 政务外网应用

3.2.1.2.2.1 宣防任务管理

以网格管理为基础，将触达任务进行流程化、网格化的部署，动态发布触达任务、跟踪触达任务、监控触达任务、协调触达任务、考核触达任务等，充分发挥网格员的力量，提升预警信息的触动率，降低案件的发生。

一、信息下达管理

基于省社管平台的数据基础，设置信息下达的层级关系、角色权限以及宣防指令下达的流程，可视化跟踪指令处置的状态和信息触达率。

1、层级角色设置

调用社管平台的人员管理体系，以菜单的形式完成对人员权限、角色层级的动态配置，实现宣防资源的动态调配。

2、下达流程配置

依据社管平台的工作流程体系，可视化设置宣防任务的下达流程，配置每个流程的节点以及节点属性和参数，并根据实际业务动态调整相关任务下达流程。

3、指令处置跟踪

对指令处置的情况进行可视化跟踪，实时掌握指令执行的状态，以列表的形式展现，并结合指令处置的情况分析信息的触达率。

二、案档文件管理

案档文件管理以文件目录的形式实现为对系统案档文件进行可视化管理，提

升案档文件的共享效率，防止案档文件遗漏和丢失，方便案档文件的移交和工作协同。

3.2.1.2.2.2 基础支撑管理

基础管理中心为应用提供系统支撑，完成与公安网、互联网的数据对接、处理数据与前置机交换、数据字典管理、宣防员管理以及接口监控等。

3.2.1.2.3 互联网应用

3.2.1.2.3.1 宣防员桌面端应用

包括信息发布、预警管理、任务管理、工作统计、工作提醒等。

信息发布：动态发布相关预警信息、工作通知等；

预警管理：管理本账号的预警宣防信息，填写宣防反馈结果；

任务管理：处理下达的指令和任务，并填写相关任务的处置结果；

工作统计：以列表的形式展现预警宣防、指令任务等工作的处理情况；

工作提醒：以系统消息的形式对需要处理的工作进行提醒，便于及时处理。

3.2.1.2.3.2 宣防员小程序

宣防小程序包括预警回访、宣防通知、线索上报、意见上报、工作统计、工作提醒等。

基于现有海南“海易办”小程序做升级开发，增加“反诈宣防”人口；功能包括预警回访、宣防通知、线索上报、意见上报、工作提醒、工作统计。

3.2.1.2.3.3 涉诈重点人员管控 APP

管控 APP 分管控负责人和被管控人员两类用户：

1、管控负责人版

管控负责人定期审核被管控人员信息。将辖区内需要对其进行布控管理的重点人员信息推送管控 APP 系统，并关联管控负责人。系统对涉诈重点人员相关信息进行统一管理。

2、被管控人员版

被管控人员安装管控 APP，定期进行报备，或按照公安机关要求上报情况等。

3、个人设置

包括显示风格、消息提醒、用户设置、密码设置、登录设置等相关人性化的设置。

3.2.1.2.3.4 基础支撑管理

基础管理中心为应用提供系统支撑，完成与省社管平台的数据对接、处理数据与前置机交换、数据字典管理、权限管理、区域管理、网格管理以及接口监控等。

3.2.1.2.4 省通信管理局协同处置子系统

3.2.1.2.4.1 系统管理模块

3.2.1.2.4.1.1 菜单管理

可对菜单进行添加根、新建菜单、修改、删除、刷新、添加权限、查询操作。

3.2.1.2.4.1.2 用户管理

1、系统前台支持单点登录，以及通过统一认证平台等方式认证登录；

2、系统登录支持图片和短信验证码等反暴力破解的功能；

3、可对用户进行查询、修改、删除、重置密码等操作。

3.2.1.2.4.1.3 角色管理

包括角色信息（列表）查询、增加角色、删除角色、修改角色等操作。

3.2.1.2.4.1.4 组织机构管理

包括组织机构信息（列表）查询、增加组织机构、删除组织机构、修改组织机构等操作。

3.2.1.2.4.1.5 登录日志管理

记录系统的用户登录情况，可以查看用户的登录账户，登录时间，登录 IP。

3.2.1.2.4.1.6 操作日志管理

记录用户对系统的操作行为，主要记录操作人 IP、操作时间、操作时长、操作的 URL、请求参数、响应参数、备注描述。

3.2.1.2.4.1.7 登录用户活跃度统计

支持对登陆用户进行活跃度统计，针对用户的登陆频次进行统计和显示。

3.2.1.2.4.1.8 使用模块热度统计

系统可以对不同用户使用的模块被调用的频度进行统计并显示结果。

3.2.1.2.4.2 协同处置模块

与省反诈信息化平台信息共享及联动处置；

与工信部反诈大平台信息共享及联动；

与属地基础电信企业（移动、联通、电信）的处置系统进行封堵策略下发和

封堵日志接收联动。

3.2.1.2.4.3 通联预警劝阻模块

需进行通联预警的涉案号码通过部省联动接口推送预警任务到工信部反诈大平台，工信部反诈大平台将预警结果反馈至省系统。

3.2.1.2.4.4 DNS 管理模块

3.2.1.2.4.4.1 违法违规域名处置

向企业侧系统下发违法违规域名处置指令，要求企业侧系统按照指令时限要求对域名进行处置后上报处置结果，协同处置子系统接收并转发到省反诈平台。

3.2.1.2.4.4.2 域名解析日志

接收企业侧系统上报的相关日志信息；能够按照关键行业管理要求，发起对相关日志的主动查询；相关法律法规明确有关日志信息留存时限的，从其规定。

3.2.1.2.4.4.3 解析记录上报

接收对所辖内全部企业侧系统主动定时上报的域名解析记录信息。

3.2.1.2.4.4.4 违法违规域名监测

能够对企业侧系统下发的违法违规域名监测指令，按照指令时限要求企业侧系统对违法违规域名进行监测，并上报监测结果到协同处置子系统，并通过协同处置子系统转发到省反诈平台。

3.2.1.2.4.4.5 疑似与异常数据处理

将收集后的疑似数据与异常数据推送给企业侧系统，企业根据下发内容进行相应本地操作。

3.2.1.2.4.4.6 数据接收及预处理

负责接收数据并对数据进行预处理。

3.2.1.2.4.4.7 数据入库功能模块

负责访问日志的批量入库、存储管理。

3.2.1.2.4.4.8 Portal 页面呈现及交互模块

负责提供 web 查询交互界面和查询结果呈现、导出。

3.2.1.2.4.5 涉诈电话处置管理模块

3.2.1.2.4.5.1 单个号码处置

系统可以对单个号码进行审核，并通过人工方式来进行手动关停处理。

3.2.1.2.4.5.2 批量号码处置

3.2.1.2.4.5.2.1 批量处置业务流程设计

批量导入需要处置的号码，同时再导入界面填写对应批量关停号码组关停通知短信内容，审核人审核通过后，开始调用短信端口对号码群发送短信通知，完成短信发送后，间隔 5 分钟，开始执行不良号码批量关停。

3.2.1.2.4.5.2.2 批量处置功能实现

- **批量处置查询**

用户可以查询该账号对应运营商已添加的批量处置任务，查询维度包括：发起人、审核人、审核状态。包括批量导出、模版下载、批量导入、详单查看等。

- **批量关停审核**

审核人账号可以查询该账号对应运营商已添加的批量处置任务，查询维度包括：发起人、审核人、审核状态。并对任务进行审核操作。

- **单个号码复开**

系统可以对单个号码进行审核，并通过人工方式来进行手动复开处理。

- **批量复开**

批量导入需要复开的号码，同时再导入界面填写对应批量复开号码组复开通知短信内容，审核人审核通过后，开始调用短信端口对号码群发送短信通知，完成短信发送后，间隔 5 分钟，开始执行号码批量复开。

3.2.1.2.4.5.2.3 违法违规电话监测

按照指令时限要求企业侧系统对违法违规电话进行监测，并上报监测结果到协同处置子系统，并通过协同处置子系统转发到省反诈信息化平台。

3.2.1.2.4.5.2.4 疑似与异常数据处理

将收集后的疑似数据与异常数据推送给企业侧系统，企业根据下发内容进行相应本地操作。

3.2.1.2.4.5.2.5 数据接收及预处理

负责接收数据并对数据进行预处理。

3.2.1.2.4.5.2.6 数据入库功能模块

负责信令及流量的批量入库、存储管理。

3.2.1.2.4.5.2.7 Portal 页面呈现及交互模块

负责提供 web 查询交互界面和查询结果呈现、导出。

3.2.1.2.4.6 数据展示模块

整体概况展示,可按月、日筛选查询、展示如下指标：恶意链接封堵数量和涉诈电话关停数量;

处置态势展示,恶意链接处置和涉诈电话处置态势展示,近 24 小时内的处置量以折线图展示;

处置量突发告警,实时分析处置量，对处置量突发增加或下降到一定比例时实时告警。

3.2.1.2.4.7 数据共享模块

省反诈平台与工信部反诈大平台通过协同处置子系统实现涉诈资源的双向共享，以便开展深度研判。本系统与工信部反诈大平台之间的数据共享主要包括涉诈资源上报、涉诈信息（线索）下发等功能。

涉诈资源上报包括：涉诈网址上报、涉诈域名上报、涉诈 APP 上报、涉诈互联网账号上报、涉诈短信上报、反诈成效统计上报。

涉诈信息下发包括：用户举报号码信息下发、公安通报号码信息下发、涉诈域名下发。

3.2.1.2.4.8 报表统计

每天对新增的恶意域名和涉诈电话进行统计;

处置统计,每天对命中恶意域名和涉诈号码的数量进行统计展示;

处置实时监控,实时展示涉诈域名和涉诈电话处置信息和态势。

3.2.1.2.4.9 接口开发及系统集成

1、与运营商侧 DNS 系统接口对接

需与各个运营商侧 DNS 系统进行对接。

2、与运营商侧电话反诈系统接口对接

需与各个运营商侧电话反诈系统进行对接。

3、与工信部反诈大平台对接

需与工信部反诈大平台对接。

3.2.1.2.4.10 系统软硬件建设需求

见附表 1

★3.2.2 行业数据联动核查管控系统

3.2.2.1 系统总体需求

行业数据联动核查管控系统的建设将全力构筑全社会参与、各单位协作的防范治理体系，进一步整合力量资源，充分发挥海南省公安厅（反诈中心）、通信管理局、中国人民银行海口中心支行、市场监督管理局等部门职能作用，提升打击犯罪整体效能，推动反诈业务重塑、模式重塑、制度重塑和服务重塑，助力社会治理体系建设，加强公安机关与银行、运营商的无缝对接，吸纳互联网企业参与深度合作。

3.2.2.2 系统功能模块需求

3.2.2.2.1 系统应用功能

行业数据联动业务场景是基于反诈生态应用架构，为公安、通管、人行、市监、银行、运营商等各反诈联盟参与方提供的反诈应用服务。

根据反诈协作的要求，提供一套标准反诈生态应用，包括协同处置、信息共享、信息核验、预警联防等不同类型应用服务。用于劝阻保护、黑灰共享、处置协同、分析打击、信息核验、联合建模、预警联动等业务场景。并根据省联席办工作规范、衔接顺畅、协作高效，构建形成上下联动、相互支撑的一体化打击防范格局。联盟各参与方可利用标准的应用服务开展反诈协作，随着反诈形势发展变化，还可以通过各联盟持续扩展应用服务建设，以满足攻防手段、成员扩展的需求

系统提供表单型、接口型、流程型三类业务，支持界面操作、服务在线调用和业务流定义，联盟单位根据各自网络和内部系统建设情况，在终端设备上自定义封装反诈业务服务并进行发布，通过灵活搭配组合表单、流程和接口等各类基础服务构建反诈生态应用。

3.2.2.2.1.1 协同处置

1、处置发起

公安机关根据案情，对涉案介质信息和处置指令进行归类分发，通过反诈联盟直达各成员单位，同时跟踪各成员单位反馈时效和接收情况。

2、处置反馈

根据公安下发的处置任务，根据流转策略至各参与机构进行任务的核处，根据任务内容以及时效要求，各单位可结合内部风控处置规则进行系统自动核处执行。

3、处置场景

处置场景包括互联网账号注销、电话号码封停、网址（域名）封堵、银行卡冻结、数据协查等。

3.2.2.2.1.2 黑灰介质共享

1、共享应用

提供公安、通管局、运营商、银行等数据协作通道，实现黑灰数据加密交换、全域共享和多方数据核验功能。

2、共享场景

共享场景包括号码信息、银行卡信息、互联网账号信息、网址信息、APP 信息、域名信息、IP 信息等。

3.2.2.2.1.3 预警联防

1、行业预警

各信源节点基于各自数据和模型识别能力感知异常开卡人员，依托公安数据和外部数据联合建模识别涉诈重点人开卡、异地来琼密集开卡、跨运营商（跨银行）超量开卡预警。通过构建多方风险联防机制，深挖开卡、卖卡、贩卡、买卡黑灰产团伙。

2、预警处置

根据预设内部预警模型以及结合外部行业数据联合建模，对高危通话预警、触网预警、高危交易预警、警情信息以及异常对公账号、异常开卡行为、开卡团伙、异常企业注册信息进行联动，并根据公安研判分析结果进行风险处置。

3、预警应用场景

预警应用场景包括涉诈高危数据、涉诈互联网风险感知、涉诈警情信息、涉

诈高危触网和高危通话、跨运营超量开卡预警、跨银行超量开卡预警、异地来琼密集开卡预警、本单位开卡异常预警、企业注册登记异常预警、对公账号资金异常预警。

3.2.2.2.1.4 信息核验

1、核验统计

按照核验服务提供方绑定服务单位分为公安侧、通信侧、金融侧、市场监督管理等，对服务调用情况、核验情况和异常核验预警进行统计。

2、核验任务发起

提供联盟各方在线数据接口能力封装能力，通过输入查询信息进行单一服务接口查询。

3、核验结果查看

根据请求相关核验服务，返回一致性比对结果（人号、地址）、状态、风险值等。

4、核验应用场景

核验应用场景包括号码信息、号码状态、地址信息、人员身份、开卡综合风险等。

3.2.2.2.2 应用功能支撑管理

基于联盟网络构建反诈应用服务管理系统，提供应用功能支撑管理用于拉通参与机构反诈生态应用服务上架发布。反诈生态应用开发模块为参与机构反诈生态应用开发者提供基础能力，合约在线管控用于构建参与方合约开发发布可视化流程，反诈生态应用快速构建和发布用于为行业单位提供快速搭建反诈生态应用提供统一技术标准。

3.2.2.2.2.1 数据模型

数据模型即为业务应用的数据存储结构以及数据关联关系。在边缘计算终端里的反诈应用数据模型分为本地数据模型和联盟数据模型。

1、本地数据模型

本地数据模型即终端的业务数据。边缘计算终端为各成员单位应用提供单独

的数据库，用于储存本地数据模型。

2、联盟数据模型

联盟数据模型即为业务应用与联盟交换的数据存储结构，包括数据下发、链上数据查询、黑灰介质共享、数据碰撞、文件共享、接口调用，交换方式以数据流转策略来定义。

根据具体的业务应用场景来选择和定义相应的策略。策略共分为三种类型，数据流转、黑灰介质共享、业务服务。

3.2.2.2.2.2 流转策略

1、协同处置策略

指需要多个反诈应用订阅方协同完成任务处置、反馈处置、追踪处置、风险识别预警等联合开展工作的业务应用场景，多方的协同数据需要通过反诈联盟链来完成流转，从一方流转到指定方或广播流转到所有订阅方。

2、黑灰介质共享策略

指要求数据在不出域的情况下进行多方共享的应用场景，通过反诈联盟链高速传输网络进行黑灰介质共享，在边缘计算终端里共享出的数据不会在数据请求端持久化，并且数据在传输过程中是以加密的方式进行传输。可以一方共享给多方，也可以一方全域共享。

3、核验服务策略

反诈应用可以通过开放一些业务接口来为订阅者提供计算结果，接口提供者会在本地通过隐私计算等方式完成计算结果，并把结果通过开放接口返回给调用端，结果在传输过程中是以加密的方式返回。可以指定多方来调用，也可以开放给所有订阅者。

3.2.2.2.2.3 反诈应用订阅/使用

1、应用订阅

提供反诈联盟行业应用服务清单，在应用服务列表中，联盟单位订阅和取消功能用于选择使用或参与开发联盟中已有应用模块。

2、应用使用

系统提供最小颗粒的原子服务能力，相关使用权限做严格控制。

3.2.2.2.2.4 反诈应用开发

系统提供此架构基础上的图形化开发工具包括应用基本信息、数据流转策略和数据存储模型，以及应用状态的创建和更新。并通过边缘计算终端进行发布，供多方进行订阅使用。

1、反诈应用创建

系统支持创建所属应用清单，如应用名称、应用 ID、应用类别，各成员单位可根据自身数据和接口情况进行定义。

2、应用基础信息

根据创建反诈应用所需要的基础信息进行内容填写，如应用名、应用 ID（自动生成）、应用类型、应用范围和订阅单位。

3、应用数据模型

系统提供自定义接口，可根据自身数据特征填写字段名称、字段类别和字段长度，通过字段组合形成应用模型数据接口。

4、应用策略

根据反诈应用的使用方式不同，支持定义“处置数据流转”“黑灰介质共享”“核查业务服务”三种不同策略类型。可根据业务流需要定制智能合约模板，系统根据流转规则自动执行，减少人工协同成本。

5、应用状态创建和更新

按照开发流程规范，对行业应用状态进行更新和创建。如草稿、测试、正式、发布状态，反诈应用自动更改为相应状态。

3.2.2.2.2.5 应用发布管理

1、应用发布

在完成反诈应用发布之后，系统提供应用发布功能，等待后台管理员审核完成之后，即可在反诈应用服务列表中看到此反诈应用服务。

2、应用关停

反诈应用由于外在原因影响继续使用，需要在服务列表中移除时，支持对反诈应用管理中的关停功能，关停后反诈应用服务列表中将无法看到此反诈应用。

3.2.2.2.2.6 反诈应用更新

当反诈应用涉及版本迭代更新时，系统提供远程更新操作，可对当前反诈应用进行模型、策略、应用包等服务的更新操作。

3.2.2.2.3 可信数据支撑管理

基于反诈联盟底座开发，实现行业各节点数据、服务整合，并借助反诈联盟链不可篡改、可追溯等特性，实现数据追溯、流转及验真，同时针对数据提供方、数据使用方分别提供了丰富的数据管理模块。

3.2.2.2.3.1 联盟链基础服务

提供反诈联盟链共识节点上链服务，包括基础模型，算法，合约，证书密钥等基础服务。

3.2.2.2.3.2 上链存证配置

采用信封加密技术，实现数据密文流转，在数据从属主方转移到使用方的过程中，将数据进行加密，确保使用方只能获得加密后的数据。结合信封加密技术，提供的密文只能被授权的使用方使用，保证数据被转移给第三方之后无法使用，从而解决了数据转卖的问题。

3.2.2.2.3.3 数据归属绑定

进行数据资产的资产归属权绑定操作，完成数据归属确权。通过接口导入批量数据并且进行数据归属权标签绑定，实现数据归属确权。

3.2.2.2.3.4 数据授权管理

数据使用方机构可进行授权操作，只允许授权机构进行数据调用使用。提供接口供数据提供单位进行数据授权，允许参与单位在特定的场景下对某些维度的数据进行访问，并在后续的数据流转时进行授权状态验证。

3.2.2.2.3.5 数据加密

为业务场景提供数据加密服务，支持数据加密流转，支持多种加密算法，包括国密算 SM2，RSA 等多种加密算法。

3.2.2.2.3.6 数据验真

提供数据验真服务，可通过 SDK 接口调用链上数据，并对当前使用数据进行对照，识别数据的真实性和正确性。

3.2.2.2.3.7 数据追溯

基于链上可信数据资产，以数据资产的 hash 为索引，对链上数据资产进行追溯查询，并以图示进行展示。

3.2.2.2.3.8 数据审计

针对链上数据流转情况提供统一的数据审计服务，对数据授权、数据采集、数据输出各个环节的关键信息提供可视化的审计服务。

3.2.2.2.3.9 数据索引目录管理

链上数据索引目录管理可对数据以资源目录的形式进行合理清晰管理，并将数据资源目录记录，生成目录链。通过不可篡改、具有唯一性的目录 hash，实现链下数据与链上存证数据之间的关联绑定。

3.2.2.2.3.10 数据索引服务

配置索引与API的对应关联关系，实现通过API对链外数据流转的统一管理。

3.2.2.2.3.11 数据采集策略配置

针对数据采集策略进行配置管理，明确数据资产源的采集类型，数据来源路径，存储方式，模型选择等进行配置。

3.2.2.2.3.12 数据流转策略配置

针对数据流转过程中需要对流转的规则策略进行配置，不同的业务场景对应不同的业务数据，不同的业务数据对应了不同的数据流转规则。

3.2.2.2.3.13 场景管理

平台为管理者提供一个统一的数据服务管理界面及入口，在该平台中，管理者可对平台相关参与方的账号进行新增、删除等操作。

3.2.2.2.3.14 机构准入管理

机构可以通过上传证书请求，申请加入某联盟链，同时对用户接入的公私钥进行管理，用户在本地生成证书请求和私钥后，需保管自己的私钥文件和密码。申请加入联盟链时，需上传证书请求，证书请求审核通过时，上传的证书请求将由 CA 中心签名。应下载签名后的证书，访问须使用签名的证书请求和私钥。

3.2.2.2.4 系统运行支撑管理

3.2.2.2.4.1 运行统计

提供监管大屏，对联盟接入单位数、应用发布数、服务调用情况、单位绩效情况等进行综合展示，直观展示联盟内数据分布、硬件资源和应用情况。

1、联盟统计

绘制联盟单位数量饼状图、行业分布热力图、终端设备分布图、应用发布折线图综合展现联盟情况。

2、数据统计

综合展现各单位应用使用情况，如数据贡献量、数据查询量、数据存证量、开放服务数，并进行单位绩效排序显示。

3.2.2.2.4.2 审批管理

对于联盟发布应用进行流程审批，审批过后应用发布联盟应用，用于各成员单位订阅使用。包括我发起的申请，待审批的申请和已审批记录。

1、我发起的申请

对于新发布应用，需要所属成员发起发布申请，由联盟管理员进行审批操作。

2、待审批申请

联盟管理员对下属成员发起的申请进行审批或驳回操作。

3、已经审批记录

通过审批的应用发布申请，进行回溯查看。

3.2.2.2.4.3 运维管理

1、终端设备管理

对终端设备 CPU、内存、硬盘、网络进行综合监控管理，便于设备故障感知和后续运维工作。

2、联盟日志行为审计

对终端访问日志和数据使用日志进行行为存证，提供数据溯源和终端行为审计功能。

3.2.2.2.4.4 成员管理

1、账号管理

设置接入单位账号体系，实现对账号的添加、删除、修改等操作。

2、权限管理

对已添加联盟账号相关权限进行配置，如服务列表、运行统计、终端查看、业务应用模块查看等。

3.2.2.2.4.5 个人中心

查看当前账户信息，并可对当前账户的基础信息和关联账号密码进行修改管理。可查看当前账户所关联的成员信息。

3.2.2.2.5 多方业务平台接入服务

3.2.2.2.5.1 公安反诈业务系统接入服务

提供公安反诈业务系统接入服务，实现联盟反诈应用与公安内部业务系统联动拉通，进一步加强数据流转的时效，减轻民警工作量。

3.2.2.2.5.2 机构业务对接服务

提供反诈参与机构业务系统对接服务，实现反诈业务应用与机构内部业务系统实时交互联动。

3.2.2.3 配套软硬件建设需求

基于反诈业务场景构建软硬一体边缘计算终端，解决联盟参与方与联盟链最后一公里。

数据模型用于构建适配用户多样化复杂场景数据结构，模型在数据广度（数据类型不多扩充）和深度（数据量大小）两个维度的不断扩展，完成构建多样化的模型能力。

省公安厅（反诈中心）、省通信管理局、省市场监督管理局、人行海口中心支行、地市公安局的 5 台边缘计算终端纳入本次项目建设采购。

硬件参数需求见附表 2

★3.2.3 侦查协作实战应用系统

3.2.3.1 系统总体需求

侦查协作实战应用系统部署在公安网内，包括联动核查数据服务、多流数据研判、在线协同办公、线索在线上报以及系统支撑管理等功能内容。

3.2.3.2 系统功能模块需求

3.2.3.2.1 联动核查数据服务

包括开发协同处置管理、黑灰介质共享管理、预警联防管理、线索核验管理等数据服务接口，通过安全交互平台与“行业数据联动核查管控系统”进行交互。

3.2.3.2.2 多流数据研判

对通讯流、资金流、网络流、信息流进行统一的管理和分析，在案件的侦查过程中，对逐步掌握的多流信息进行入库管理，不断的充实和完善现有案件的多流信息，将多流信息与人员信息进行绑定，最终实现案件的多流分析结果。

3.2.3.2.2.1 数据智能导入

基于机器学习能够实现通讯流向数据的导入，并能实现自动学习文件格式和字段内容，解决了格式和内容导入难的问题。为智能分析模型提供数据支撑。

3.2.3.2.2.2 数据分析模型

1、多流合一分析

将人、案、地、物等相关信息进行汇聚治理、统一管理，运用大数据分析技术梳理案件线索、关联信息等。

2、通话轨迹分析

通话轨迹分析指定时间段内，目标号码的通话轨迹，并在地图上进行可视化的展示。

3、通联规律分析

通话规律分析指定时间段内，单个电话号码的通话规律。对目标号码的通话规律进行智能分析，并以图表的形式。

4、通联时序分析

对案件相关的多个话单进行智能时序分析，梳理通话时间与案情发展的脉络。

5、通联关系分析

对案件相关的所有话单进行智能分析，通过通讯关系、通话次数、通话时间等深度挖掘涉案人员的通讯关系，展现可视化的关系网络。

6、资金流向分析

通过对目标账单的交易情况进行智能分析完成对资金的流向的溯源。

7、资金流特征分析

结合资金流向分析规则，分析来源卡、中转卡和去向卡等特征。

8、团伙关系分析

通过对多个关键要素比对分析，建立团伙关系图，梳理出涉案团伙中重要的成员。

9、地下钱庄分析

建立地下钱庄分析模型，配置模型参数和权值；通过多项特征的计算，分析出地下钱庄卡。

3.2.3.2.3 在线协同办公

借鉴互联网协同办公的模式，通过即时通讯、文档协同等模块在公安网内实现办案民警之间的高频次的在线协作与交流。包括：消息提醒、目标页面链接、在线交流工具、文档协作、脑图协同、挖掘协同、在线绘图等。

3.2.3.2.3.1 文档协同

在线创建 Excel、Word、PPT，在线文档编辑，线上文档保存到本地、个人文件管理、文件共享以及多人之间的文档协作，多人在线共同编辑，达到文档协同编辑。

3.2.3.2.3.2 脑图协同

提供创建思维导图的功能，通过思维导图的展现形式，结合系统操作者使用思维导图的操作习惯，将研判思路通过思维导图的形式进行呈现。

3.2.3.2.3.3 挖掘协同

提供关系图分析功能，通过将线索作为入口进行的数据挖掘、分析和串并等过程，逐层关联递进，结合节点之间的连线，形成数据间的关系网络，最终结果以关系网络图的形式展现并且可以导出。

3.2.3.2.3.4 即时聊天

开发系统内部的在线交流工具，在协同侦查时以即时通讯来满足在线交流的

工作需求，并集成到文档协同中，方便再文档协同时进行即时的信息沟通。

3.2.3.2.3.5 在线绘图

提供便捷的绘图工具，工具提供一个在线的画布和一些基本的画图图形，可以自由发挥画自己需要的图形。

3.2.3.2.4 线索在线上报

定制采集模板，并按照采集模型完成线索在线上报工作。

支持各地市、区县线索的录入、上报、撤回、管理及统计分析等业务应用，支持对线索的上报数量进行统计分析，可视化展示。

3.2.3.2.4.1 上报类型管理

动态管理上报类型，支持增加、修改、删除上报类型；例如，上报的线索信息主要包含以下线索：

3.2.3.2.4.2 上报任务管理

系统支持对已上报的情报线索数据进行集中管理、查询、展示。

通过发起上报，上传情报线索信息，以列表形式展示情报线索数据的上传信息，支持对我上传的情报线索查询、撤回及详情查看。

系统实现对情报线索信息的管理，通过列表的形式进行展示，支持对情报线索批次查询及详情查看。

3.2.3.2.5 系统支撑管理

3.2.3.2.5.1 综合信息服务

1、超级链接

应用导航模型提供常用的系统超级链接，通过集成整合各应用系统链接，可以快速访问指定系统。

2、超级搜索

集成相关业务应用系统已开放的查询接口，设置一站式查询入口，无需切换指定系统进行查询，提高工作效率。

支持选择搜索条件进行数据多维搜索。

支持在搜索框中输入一次关键字及可完成数据智能化搜索。

2.2.3.2.5.2 数据资源服务对接

系统对接汇聚国家反诈大数据平台、公安大数据实战平台、反诈预警综合分析系统、刑专系统、海南省打击电信网路诈骗犯罪合成作战平台(一期)以及第三

方数据等对接。另外，系统开发离线数据和历史数据导入接口，完成离线数据和历史数据对接。

3.2.3.2.5.3 业务质量检测

对数据录入格式和业务处理质量的自动检测，主要包含接警模块和预警回访模块的质量检测。

1、警情质量检测

系统支持对接警业务处理和业务流转的质量检测。

系统支持对案件涉及的通讯流、资金流、网络流等信息流进行应采未采信息质量检测。

系统支持对警情信息录入字段的格式进行质量检测。

2、预警回访质量检测

系统支持根据预先设定的符合数据分发相关质量检测规则。

系统支持根据预先设定的符合人工回访相关的质量检测规则。

系统支持根据预先设定的符合上门回访相关的质量检测规则。

系统支持对预警回访业务处理的质量检测。

系统支持根据预先设定的符合数据准确性相关的质量检测规则。

3.2.3.2.5.4 系统管理

账户权限管理：包括用户管理、角色管理、授权管理

个人工作台：提供个人信息维护及个性化设置功能。

绩效监督考核：包括考核指标设计、考核指标配置以及考核指标与任务流转、业务操作等工作进行集成。

操作日志管理：系统自动统计用户的操作日志，并以列表的形式展示操作日志。

系统运维管理：可视化系统运维管理，包含对程序内存监控、服务器监控、请求跟踪、磁盘监控、SQL 监控等。

3.2.4 性能需求

平台系统必须有很强的健壮性，不能因为大量用户并发使用而造成系统崩溃；具体功能应满足的性能要求如下表所示：

功能划分	响应时间要求
数据采集	可以按照一定格式，自动提取信息，并进行数据完整性、合法性检查；处理时间<5 秒
数据保存	数据入库的速度<15 秒
查询检索	简单查询响应速度<3 秒；复杂和组合查询响应速度<30 秒；能够对相关文件进行检索、模糊查询；查询结果可以按照一定原则进行排序、筛选、保存；查询结果可以显示为图形或图表，可以输出到通用的办公处理软件中。
报表输出	报表输出相应时间<10 秒，并有进度显示；动态表处理时间<30 秒，并有进度显示。
权限管理	根据用户类别，划分角色和权限。处理时间<5 秒钟
系统日志	系统运行日志应记录对系统数据的修改、访问日志；可以定期清理；数据库应当有日志文件，以做备份恢复。处理时间<5 分钟

四、项目实施及服务

1、项目实施期限

签订合同后 12 个月内完成系统建设工作。**如投标人未能按期完成，将按日承担延期违约金，投标时提供“项目按期完成承诺书”，格式和内容自拟。**

交货地点：用户指定地点。

2、系统维护及培训

中标方需在系统验收后提供不少于 3 人的驻场服务团队，在符合公安部相关接口标准的前提下，根据采购方业务和发展的需要，免费提供系统接口，积极配合采购方进行系统的对接和调试工作，确保系统的持续研发和稳定运行。

中标方需提供 7*24 小时响应服务，保证在接到故障电话后响应时间小于 1 小时，在 48 小时内解决问题。系统免费维护期为 3 年（自通过系统终验起计算）。

中标方对使用单位人员进行技术培训，包括集中培训、现场培训。培训内容为系统使用方法和技巧，故障诊断，维护管理等方面，使之能适应系统正常运行的需求，培训的时间、方式、参训人员由采购方确定和组织，培训所需的讲师费

用、教材费用由中标方承担。

五、其他要求

1、投标商须保证所提供软件不涉及任何知识产权纠纷。

2、需融合和应用海南省打击电信网路诈骗犯罪合成作战平台(一期)建设的数据和应用成果，**投标方需提供“对接和应用海南省打击电信网路诈骗犯罪合成作战平台(一期)建设应用成果”的承诺书和对接应用方案（包括但不限于技术实现、部署实施、实现能力证明材料等方面），格式和内容自拟**。

3、采购需求中标注“★”号的功能为本项目重点建设的核心功能，但不作为无效投标条款。

4、投标方须提供针对本项目的详细技术实现和售后服务方案，根据招标技术需求提供相关技术材料，该材料作为招标和验收的依据之一，不能撤回。

5、演示要求

对“系统规格及技术要求”中标记“★”号的核心功能进行现场演示讲解，具体要求如下：

序号	演示项名称	需演示的具体内容及功能	演示结果
1	行业数据联动核查管控系统-应用开发	①应用创建（应用基础信息+应用类型+应用标签+应用描述+数据模型定义+业务流转策略）； ②应用发布管理（应用测试+开发联调+应用发布+应用下线+应用远程更新+应用订阅部署）。	□成功演示 □未成功演示
2	行业数据联动核查管控系统-运维管理	①设备状态监控查询； ②运维分析日志查询； ③应用状态监控查询。	□成功演示 □未成功演示
3	行业数据联动核查管控系统-联盟链基础服务	①联盟链创建（创建联盟链-创建证书-创建账户-合约开发）； ②证书管理（创建证书-密钥密码-下载根证书）； ③合约管理（智能合约内容-生效范围-合约 ABI 上传-原生存证模型定义）； ④节点管理（新增节点- License 授权-添加域外节点-节点启停-节点配置）。	□成功演示 □未成功演示

4	行业数据联动核查管控系统-数据共享流转	①数据采集（基础信息-数据来源配置-数据清洗配置-加密算法-数据存储配置）； ②数据流转（基础信息-流转策略-输出模型配置）； ③数据追溯（数据资产化-hash 查询-授权链路查看）。	□成功演示 □未成功演示
5	侦查协作实战应用系统-文档协同	①在线创建、编辑 Excel、Word、PPT； ②线上文档保存到本地； ③在线上传本地 Excel、Word、PPT 文件； ④文件共享以及多人之间的文档协作，多人在线共同编辑。	□成功演示 □未成功演示
6	侦查协作实战应用系统-脑图协同	①在线创建、编辑脑图文件； ②线上脑图文件保存到本地； ③在线上传本地脑图文件 (支持.km、.json、.md 格式)； ④脑图共享以及多人之间的脑图协作，多人在线共同编辑。	□成功演示 □未成功演示
其他	**现场演示温馨提示说明**	**（1）现场演示准备** **投标人自行准备演示所需软件、数据以及设备、网络等演示环境。** **（2）演示方式** **投标人通过实际系统或系统原型的方式进行现场讲解演示，其他形式无效。** **（3）演示时限** **投标人必须在 20 分钟内完成所有演示内容，到时即刻退场。** **（4）进场参与演示的人员规定** **因省公共资源封闭区场地管理，进场参与演示的人员数量最多不超过二人。**	

六、附录

附表 1：

序号	设备名称	设备说明	单位	数量
1	接口服务器	2*10 核 CPU/128G 内存/ 2*900G SAS+3*4TB SATA/4 口千兆网卡+4 口万兆网卡/支持 Raid5 卡/双电源	台	3
2	应用服务器	2*10 核 CPU/128G 内存/ 2*900G SAS+3*4TB SATA/4 口千兆网卡+4 口万兆网卡/支持 Raid5 卡/双电源	台	1
3	处置服务器	2*10 核 CPU/256G 内存/2*900G SAS +6*4TB SATA/4 口千兆网卡+4 口万兆网卡/支持 Raid5 卡/双电源	台	4
4	核心交换机	双电源模块，≥48 个 10/100/1000BASE-T 端口，≥24 个 SFP+端口，千兆光模块≥12 个，万兆光模块≥12 个，QFSP 端口≥2 个，双电源，具备堆叠功能，可提供扩展槽	台	2
5	辅材	跳纤、网线、水晶头、线槽、扎带等辅材	批	1
6	下一代防火墙	支持入侵防御、防病毒检测与阻断等功能。支持将任意接口数据完全镜像到设备自身的其他接口，用于抓包分析。网络处理能力≥10G，并发连接≥260 万，支持每秒新建连接 18 万/秒， 冗余电源，10/100/1000M 自适应电口≥6 个，万兆光口数量≥4 个，万兆光模块≥4 个，支持扩展槽；支持液晶屏，含入侵检测模块。含三年授权	台	2

7	漏洞扫描系统	Web 扫描域名无限制，Web 扫描任务并发数≥15 个域名。系统扫描 IP 地址无限制，支持扫描 A 类、B 类、C 类地址，系统扫描支持至少 100 个 IP 地址并行扫描。硬盘≥1T，千兆 10/100/1000M 自适应电口≥6 个，扩展插槽≥2 个,液晶面板显示，USB 口≥2 个，具备 Console 口。	台	1
8	日志审计系统	冗余电源，专用千兆硬件平台和安全操作系统，千兆电口≥6 个，具备管理口，USB 口≥2 个。审计对象授权≥30 个。	台	1
9	堡垒机	支持 6 种以上数据库审计与协议分析，支持添加一台或多台协议代理服务器，分担审计中心性能压力；支持 HA 双机热备；支持 oracle、postgresql、sybase、mysql、sqlserver 数据库下行返回行数和 oracle 数据库变量绑定。采用专用千兆多核硬件平台和安全操作系统，外观：标准机架式，千兆电口≥4 个,板载具备 1 个管理口 mgt，具备一个 HA 口,USB 口≥2 个,具备一个 console 口，支持口扩展槽位，硬盘≥6TB，具备冗余电源，支持液晶屏，支持≥600 路图形会话或≥1500 路字符会话并发。授权被管资源数≥100 个。	台	1

10	网络安全审计	1、SFP 千兆光接口≥2 个，千兆光模块≥2 个，千兆电口≥6 个，扩展插槽≥1 个 ； 2、IPV6 支持：支持 3、包转发率：入库速率≥32000 条/秒 4、日处理事件数： ≥2000 万条 5、网络协议支持：HTTP，HTTPS，SMTP，POP3，RDP，VNC，Telnet，Rlogin，SSH，NFS，Netbios，FTP，SFTP，SCP，Radius 等。	台	1

11	服务器密码机	1、遵循 GM/T 0030-2014《服务器密码机技术规范》、GM/T 0059-2018《服务器密码机检测规范》； 2、满足《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中“应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性”的要求； 3、支持 SM1、SM2、SM3、SM4 等国产密码算法； 4、具有商用密码产品认证证书； 5、密钥生成与管理：支持对称与非对称密钥的生成及管理，采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的真随机数； 6、密钥的安全存储：设备内可存储至少 100 对 SM2 密钥对，并且私钥部分受系统保护密钥的加密保护; 7、数据加密和解密：支持 SSF33 算法、SM1 算法和 SM4 算法的数据加密和解密运算； 8、支持管理员、审计员、操作员三权分立：分别赋予不同的操作权限，并采用数字签名技术，实现对登录用户的强身份认证。	台	1

12	签名验签服务器	1、遵循 GM/T 0029-2014《签名验签服务器技术规范》、GM/T 0060-2018《签名验签服务器检测规范》； 2、满足《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中“保证信息系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性” 3、支持 SM2、SM3 等国产密码算法； 4、具有商用密码产品认证证书； 5、签名验签服务器是集成了专门的密码软硬件模块、进行签名验签运算的服务端设备，为应用提供基于数字证书的数字签名、验证签名等服务，以保证业务信息的真实性、完整性和不可否认性。	台	1
13	时间戳服务器	1、遵循 GBT 20520-2006《信息安全技术 公钥基础设施 时间戳规范》； 2、满足《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中“应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性” 3、支持 SM1、SM2、SM3、SM4 等国产密码算法； 4、具有商用密码产品认证证书； 5、时间戳服务器采用精确的时间源、高强度高标准的安全机制、能够为用户提供精确的、可信赖的且不可抵赖的时间戳服务。	台	1

附表 2：

边缘计算终端硬件参数需求如下：

CPU 类型	Hygon C86 7265 *2
内存容量	总配置内存：256GB
磁盘容量和类型	配置 2 块 240G OS 盘 SATA SSD ，配置 4 块数据盘 1.92T SATA SSD
网卡	配置 1 块板载双口 i350 千兆，配置 1 块双口万兆网卡
电源	配置 2 个 1300W 热插拔冗余电源，电源能源的转换效率≥92%。配置 N+1 冗余易插拔风扇。
接口	配置 2 个 VGA 或者 DP 接口（其中 1 个在前面板）、 配置 6 个 USB 2.0 或者 3.0 接口
密码卡	配置具备国密商用密码产品三级资质的硬件密码卡，采用符合国密资质的安全密管芯片生成和存储密钥。

附录 配套软硬件申请情况

1、信息触达宣防管理系统

公安网侧的应用系统硬件支撑利用现有公安大数据平台的硬件资源。

以下为申请由公安厅科通处提供的公安网硬件资源清单：

序号	服务器用途	数量	服务器配置	操作系统
1	业务应用服务器	2 台	CUP：8 核， 内存：32G， 硬盘：500G	Centos7
2	数据库服务器	2 台	CUP：8 核， 内存：64G， 硬盘：2T	Centos7

政务外网侧、互联网侧的应用系统硬件支撑利用现有社管平台的硬件资源。

以下为申请由社管平台提供的资源清单：

政务外网				
序号	服务器用途	数量	服务器配置	操作系统
1	业务应用服务器	1 台	CUP：8 核， 内存：32G， 硬盘：500G	Centos7
2	数据库服务器	1 台	CUP：8 核， 内存：32G， 硬盘：1T	Centos7
互联网				
序号	服务器用途	数量	服务器配置	操作系统
1	业务应用服务器（外网 IP）	1 台	CUP：8 核， 内存：32G， 硬盘：500G	Centos7
2	数据库服务器（外网 IP）	1 台	CUP：8 核， 内存：32G， 硬盘：1T	Centos7

2、行业数据联动核查管控系统

本期项目反诈联盟基础平台、数据服务系统、应用管理系统、联盟运营系统建设需申请政务网资源进行搭建实施。

申请由社管平台提供的资源（政务外网）如下：

序号	服务器用途	数量	服务器配置	操作系统
1	联盟链基础应用服务器	4 台	CPU：8 核， 内存：32G， 硬盘：1T	Centos7
2	可信数据应用服务器	4 台	CPU：8 核， 内存：64G， 硬盘：2T	Centos7
3	业务应用缓存服务器	1 台	CPU：8 核， 内存：32G， 硬盘：500G	Centos7
4	负载均衡	1 台	CPU：8 核， 内存：64G， 硬盘：500G	/

3、侦查协作实战应用系统

应用系统硬件支撑利用现有公安大数据平台的硬件资源。

以下为申请由公安厅科通处提供的公安网硬件资源清单：

序号	服务器用途	数量	服务器配置	操作系统
1	业务应用服务器	4 台	CUP：8 核， 内存：32G， 硬盘：500G	Centos7
2	支撑引擎组件服务器	4 台	CUP：8 核， 内存：32G， 硬盘：500G	Centos7
3	作业计算服务服务器	4 台	CUP：8 核， 内存：32G， 硬盘：500G	Centos7
4	数据库服务器	2 台	CUP：8 核， 内存：64G， 硬盘：2T	Centos7