服务需求

一、背景与现状概述

（一）项目背景

根据公安部公安信息化战略部署，国家持续推进公安数字化转型，明确要求构建“专网为主+公网补充”融合通信体系，以提升全警种协同作战能力。第三代公安指挥中心建设方案（2024 年）明确提出需整合公专网资源，构建“智能协作、安全可控”的通信体系，支撑智慧警务发展。

在 2021 年 3 月，为推进全国 PDT 省省互联，“全国一张网”进程，公安部科信局分长三角地区、泛珠三角地区、成渝地区双城经济圈三个片区，部署 9 个省市探索 PDT“全国一张网”解决方案。次年，建设完成跨省互联中心，并完成互联测试。根据公安部相关工作部署，上海市局亟需建设一套跨省互联中心，满足与其他省份（包括长三角邻省）的互联互通，助力“全国一张网”建设。

（二）建设现状

目前上海 PDT 系统已实现全市 95%以上的地面道路信号覆盖，但是仍有很多室内区域仍存在信号盲区（例如场馆、商场、楼宇、地下空间、住宅等），在这些区域民警的无线通信受到限制，影响业务开展；目前上海全市的 4G/5G 运营商公网信号覆盖已非常完善，各类室内/场所基本均已覆盖运营商网络，利用运营商 4G/5G 网络来作为 PDT 信号补充，在无 PDT 信号的室内区域，通过公网继续保障民警的呼叫通

信。

另外，目前上海市公安局建设的 PDT 系统已通过 PSIP 协议与公安部实现了 PDT 系统互联，但与全国其他省份（包括长三角邻省）均未实现省省互联。亟需建设 ICC（Inter-province Connection Center，跨省互联中心），加快公安 350 兆警用数字集群通信系统全国联网的进度，助力全国 PDT 一张网建设。

（三）编制依据

本项目应符合（但不仅限于）以下所列的标准、规范及文件所涉及的相关要求:

公安部《关于推进公安信息化发展若干问题的意见》(公通字〔2017〕7 号）

《公安信息化建设“十四五”规划》

《警用数字集群（PDT）通信系统与警务辅助人员公网对讲（P-PoC）系统互联互通技术规范》征求意见稿

《警务辅助人员公网对讲（P-PoC）系统通用技术要求》征求意见稿

《警务辅助人员公网对讲(P-PoC)专用终端通用技术要求》征求意见稿

《警务辅助人员 P-PoC 技术及专用终端通用技术规范（试行）》

GA/T 1056-2013《警用数字集群（PDT）通信系统总体技术规范》

GA/T 1057-2013《警用数字集群（PDT）通信系统空中

接口物理层及数据链路层技术规范》

GA/T 1058-2013《警用数字集群（PDT）通信系统空中接口呼叫控制层技术规范》

GA/T1364—2017《警用数字集群（PDT）通信系统互联技术规范》

GA/T 1365-2017《警用数字集群（PDT）通信系统网管技术规范》

公安部 PDT 系统 M2,M3 互联操作规范协议

警用数字集群（PDT）通信系统跨省互联中心技术规范（试行）

警用数字集群（PDT）通信系统跨省互联中心技术规范（试点）

关于继续推进 PDT 省省联网试点工作的通知（公科信传发〔2022〕25 号文件）

二、目标与任务

（一）总体目标

（1）建设 1 套 P-PoC 公专网融合系统

本次建设 1 套 P-PoC 公专网融合系统，实现 PDT 信号补盲，保障民警在室内、场馆、地下等封闭区域的无线通信；提升警务协同效率，遵照公安部 P-PoC 技术规范要求，打破民警与辅警、不同警种间的通信壁垒，实现语音、定位、短消息等功能的统一调度，支撑扁平化指挥模式。

（2）建设 1 套 ICC 跨省互联中心

按照“统筹规划、统一标准、分级建设、科学管理”的原则，通过建设 1 套 ICC 跨省互联中心实现全国各地市公安跨区呼叫、自动漫游等功能，构建全国 PDT 系统公安数字无线通信“一张网”。

（3）健全安全管理措施

建设 1 套安全边界，实现风险有效控制，防止外部攻击入侵、精细化访问控制、数据信息不泄露，助力 P-PoC 公专网融合通信系统的建设与运行。

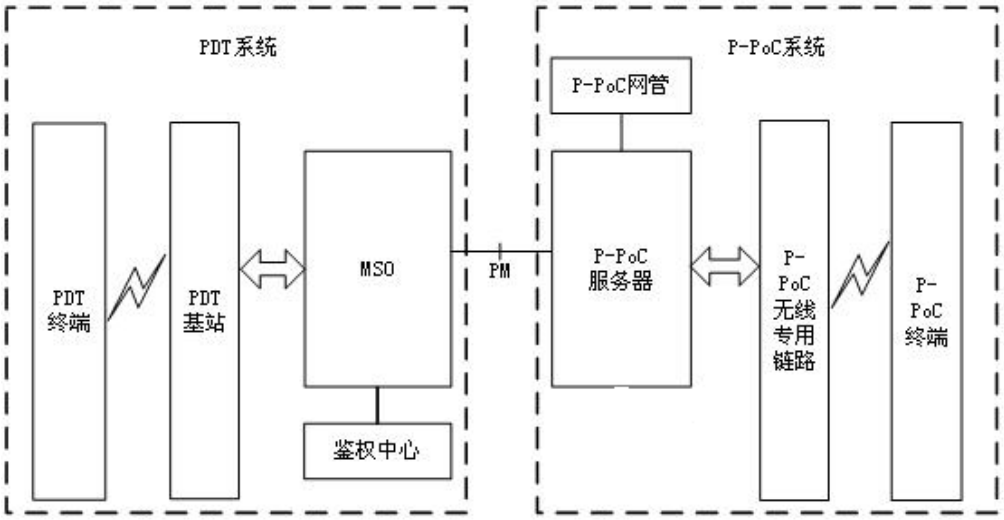
建设 1 套安全加固系统，实现加强 PDT 系统安全防护能力：提升 PDT 系统网络面对攻击、侵入、干扰、破坏和非法使用以及意外事故时的防范应急能力，提高 PDT 网络安全检测能力、防御能力和审计能力，使 PDT 网络处于稳定可靠运行的状态，保障 PDT 网络数据的完整性、保密性、可用性的能力。建立全面、可靠、完整的安全维护和管理机制。

（二）主要任务

（1）建设 P-PoC 公专网融合系统

建设 1 套符合公安部 P-PoC 标准规范的 PDT 的 P-PoC 公专网融合系统，支持国产商密算法，支持公安部标准鉴权加密功能，该系统通过标准 PSIP 协议与 350 兆警用数字集群 PDT 系统互联互通，充分利用现有的 4G/5G 运营商网络资源，实现公网 PoC 与 PDT 信号的互补，实现公专网络的融合，确保民警在执行任务现场的无线通信畅通无阻。

P-PoC 公专网融合通信系统的整体框架:



（2）建设 ICC 跨省互联中心

建设上海市统一的 PDT 系统联网网关，实现公安部与上海市 PDT 无线语音指挥调度功能，满足统一指挥需要、实现与全国其他省份 PDT 系统的互联互通，PDT 终端在跨省 PDT 系统内的自动漫游功能。

（3）健全安全管理措施

建设安全边界的主要任务是建立安全、可控、高效的互联互通机制，确保数据能在差异化的网络环境间正确、完整且受保护地流动。实现物理与逻辑连通、部署访问控制与流量过滤、保障数据传输安全、防范各类网络攻击、建立可审计和可追溯机制等。

建设安全加固系统的主要任务是通过满足安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理五个方面基本技术要求进行技术体系建设，既可以满足等级保护的相关要求，又能够全方面为警用数字集群（PDT）

通信系统提供立体、纵深的安全保障防御体系，加强 PDT 系统整体的安全保护能力。

三、建设方案

（一）建设内容

（1）P-PoC 公专网融合系统

建设 1 套 PDT 的 P-PoC 公专网融合系统(含网关服务器)，集群部署方式，实现实现对 P-PoC 的指挥调度。

（2）ICC 跨省互联中心

建设 1 套跨省互联中心 ICC（含网管中心）。负责上海市内 MSC 与省外 MSC 的呼叫控制信令的处理和语音媒体数据的转发。

（3）安全管理措施

1）建设 1 套安全边界设备，包括防火墙、交换机、语音安全传输控制系统前置机、语音安全传输控制系统后置机和安全隔离网闸，设置于 P-PoC 网络与 PDT 网络之间。

2）建设 1 套安全加固设备，包括防火墙、终端安全防护 EDR、入侵检测、漏洞扫描、数据库审计、日志审计等。

（二）总体要求

本项目所采购的设备应符合公安部所要求的技术标准，相关性能指标不得低于本需求书的参数标准，且能满足用户方指定应用开发需求。

投标人所投标的设备应是全新产品，并配备其全部功能

及相关授权，不应存在额外付费功能，如后期产品拥有新的软件版本及功能升级，投标人需根据用户要求，免费提供相应版本和功能升级服务（投标人及设备制造商应对此提供书面承诺及说明）。

投标人应提供完整的售后维保服务，包括（但不仅限于）提供 7×24 小时电话技术支持、专业维保团队、36 个月设备原厂免费保修、终身维修服务等。

四、技术性能指标及配置要求

（一）P-PoC 公专网融合通信系统

建设 P-PoC 公专网融合通信系统，实现“专网为主+公网补充”融合通信体系，以提升全警种协同作战能力，构建“智能协作、安全可控”的通信体系，支撑智慧警务发展。

序号	名称	配置要求	数量
1	P-PoC 公专融合通信系统	1.▲系统支持与 PDT 系统采用 PDT 互联标准所规范的 P-SIP 协议互联，支持集群对讲功能。 2.▲提供所投的 P-POC 公专网融合通信系统产品与国内至少一个警用数字集群（PDT）联盟厂家互联互通的盖章证明文件。 3.▲提供系统相关材料，包括软件著作权证书/检测报告/产品彩页等原件彩色扫描件加盖公章。 4.支持微服务架构，便于功能扩容/软件升级；需满足集群方式部署（三台服务器或以上），确保系统具有高可靠性。 5.系统支持 PDT 标准所规范的 CPS-P3 拨号规则和组属性（包含背景组、响应组、参与组），支持将宽带终端加入原有 PDT 窄带系统的组内，实现宽窄带终端同组互通。 6.跨系统传输的语音编解码支持 NVOC 声码器。 7.系统功能应满足《警务辅助人员公网对讲（P-PoC）系统通用技术要求》、《警用数字集群（PDT）通信系统与警务辅助人员公网对讲（P-PoC）系统互联互通技术规范》的内容功能标准要求，包括但不限于登记、去登记、鉴权、语音组呼、语音单呼、短消息、状态消息、紧急呼叫、广播呼叫、遥晕、复活、视频单呼、视频组呼、视频推送给组、视频转发给组、视频推送给单终端、视频转发给单终端、视频上拉、视频回传、多媒体消息、动态重组、报警、环境截听、环境侦视、插话、	1 套

		强拆、截听、值守、卫星定位信息传输、组呼并入、组呼迟入、在线状态呈现。 8.系统具备话权申请、话权授权、话权排队等话权处理功能,支持对普通组、公专混合组和跨系统组的创建、删除,以及组成员的增加、删除管理。 9.系统支持 TF 卡硬加密，支持 ARC4、AES128、AES256 软加密。 10.系统支持 ESN 校验，终端在进行宽带语音注册时，系统可对终端的 ESN、SN 序列号、个号进行校验。 11.系统支持终端位置信息周期上报，最小上报时间周期可达 1 秒。 12.支持对接 P-PoC 系统，支持与市局已建设的调度系统对接，实现 P-PoC 系统的接入与调度。主要包括信令解析、信令交换、呼叫处理控制、接入协议等功能。 13.单套 POC 系统最大允许开户用户数不低于 50000（集群部署）。 14.单套 POC 系统最大允许同时在线用户数不低于 20000 个。 15.单套 POC 系统最大允许开户群组数不低于 30000 个 16.单套 POC 系统最大允许组成员个数不低于 2000 个。 17.单套 POC 系统最大允许语音并发呼叫数量不低于 4000 路。 18.P-PoC 系统语音组呼建立时间应不大于 500ms。 19.P-PoC 系统话权申请时间应不大于 450ms。 20.P-PoC 系统语音传输时间应不大于 300ms。 21.P-PoC 与 PDT 系统跨系统语音组呼建立时间应不大于 700ms。 22.P-PoC 与 PDT 系统跨系统话权申请时间应不大于 650ms。 23.P-PoC 与 PDT 系统跨系统语音传输时间不大于 500ms。	
2	网关服务器	1.尺寸：≤2U，机架式； 2. CPU：≥2.4GHz 16C； 3.内存：≥64GB； 4.硬盘：≥5*600GB SAS 10K 2.5； 5.电源：220V 交流，冗余电源； 6.RAID 卡：含 4G 缓存 RAID 卡，支持超级电容； 7.满足 P-PoC 公专网融合通信系统通过该网关服务器接入市局已有的调度系统，实现对 P-PoC 的指挥调度；	1 套

（二）ICC 跨省互联中心

建设 ICC 跨省互联中心为全国公安机关跨地区调度指挥、跨区域快速调警、跨部门协同作战提供安全、可靠、高效的无线通信保障，具体体现在以下三个方面:

1、自动漫游，无缝切换

全国各地市警用数字集群（PDT）通信系统在语音上完成互联互通，各地市、县区的无线对讲终端（包括手持台和车载台、基地台）在全国范围内能够顺畅的通信，做到自动漫游、无缝切换。当终端漫游到其它地市的PDT系统下，无需任何操作即能安全快速入网，无论是与原单位同事还是支援地民警都能够顺畅通话，即能及时向原上级汇报情况也能及时接受支援地新领导的安排，做到更加高效的开展异地处警任务。

2、统一管理，权限配置

加强公安部对下辖各级公安机关的无线通信系统的监管力度，实现公安部监控中心对各省网络管理平台的管理，将管理成本降至最低，同时提高信息上报的工作效率和数据的准确性。

3、分层指挥，联动调度

在语音与数据管理联网的基础上，建立分层级（纵向）联动（横向）的指挥调度体系，实现统一协作的指挥调度模式:

1) 纵向可以实现最高指挥层直接指挥到基层，完成指挥调度的扁平化建设，基层人员可以向上级单位反馈信息，完成二次接警；最高指挥层也可以分层级布置任务，业务部门各司其职，上传下达、政令通畅。在日常应用中主要作为点名和通知的手段，在应急情况下可以快速建立指挥体系。

2) 横向可以提高平级部门间的通信联动效率，一线与一线、警种与警种、局与局在应急联动时可以快速互通，加

快信息共享的速度。

序号	名称	配置要求	数量
1	ICC 互联平台服务器	1、CPU：≥12 核 2.1GHz； 2、内存：≥16GB； 3、硬盘不低于：5*600GB 10K SAS 2.5； 4、网卡：≥2 个千兆口； 5、电源：≥2*550W AC； 6、支持 RAID 卡 ≥2GB；	2 套
2	ICC 跨省互联中心软件（含加密狗）	1）设计原则 为了使系统达到高质量、高性能、高可靠性等要求，系统建设坚持以下原则： 兼容性 上海市公安 ICC 跨省互联中心符合公安部发布的相关技术标准，能够兼容所有符合标准的终端，确保在完成建设后，不影响现有 PDT 系统正常业务。 可靠性 上海市公安 ICC 跨省互联中心可靠性体现在强大的容错能力上，当系统软件出现故障时，不会导致整个系统的崩溃，能够保障系统的整体可靠。 先进性和前瞻性 结合上海市实际情况，依据公安部相关标准规范，同时充分考虑科学技术的迅猛发展趋势，应用国内先进技术保证系统各项功能的实现；应用功能设计科学合理，符合实际应用需求；软件可根据实际需求灵活进行修改升级，同时具备强大的对接能力。 ICC 跨省互联中心负责上海市内 MSC 与省外 MSC 的呼叫控制信令的处理和语音媒体数据的转发。 1）基本要求 1、满足公安部《警用数字集群（PDT）通信系统省省联网技术方案》。 2、▲能够与上海市公安局现有 PDT 核心网系统无缝对接，完成 PDT 系统省省互联功能，投标文件中需提供无缝对接承诺书。 3、▲应提供通过第三方检测机构的检测报告，须符合警用数字集群（PDT）通信系统跨省互联中心技术规范的功能要求，提供检测报告扫描件。 （2）性能要求 性能指标：传输网络指标，用于 PDT 互联的 IP 网络满足以下性能指标要求： 1、ICC 间的链路传输时延小于 150ms； 2、ICC 和 MSC 间的链路传输时延小于 50ms； 3、传输抖动小于 25ms,丢包率小于 10^{-3}； 4、每话路带宽不小于 64kbps； ICC 性能指标，ICC 满足以下性能指标要求：	1 套

		1、跨 ICC 后组呼建立时间：小于 800ms； 2、跨系统卫星定位订阅量不小于 5000 个； 3、并发呼叫数（包含截听）不小于 1000 路。 3）联网应用功能要求 通过部署 ICC 实现省省互联互通后，应满足以下联网功能要求： 漫游登记、单呼、组呼、组呼越区切换、紧急呼叫、广播呼叫、数据业务（短消息、状态信息）卫星定位业务、旋钮组附着、截听、强拆、强插、开关机信息订阅。 1、漫游登记：漫游登记是指漫游移动终端向漫游系统发起入网请求，漫游系统确认移动终端状态和位置信息的过程。漫游系统确认移动终端身份及服务权限后方可为移动终端提供服务。 2、跨系统单呼：跨系统单呼指的是跨系统半双工单呼，是点对点的双向语音呼叫。通话建立后双方不能同时讲话，同一时间一方讲话时，另一方不能讲话只能听。跨系统单呼支持自动摘机（OACSU）和手动摘机（FOACSU）两种模式。 3、跨系统组呼：多个移动终端用户（可以包含调度台）之间相互通话的呼叫。一个组成员发起呼叫，其他组成员加入并参与通话，是一种一对多的半双工语音呼叫业务。通话过程中只能有一个人讲话，且只有主叫方可以结束呼叫。 系统根据呼叫组对组成员的重要程度分为背景组（隐含组）、响应组和参与组。 背景组：重要性最高，默认不显示在移动终端的组呼列表中。移动终端可以接收所有背景组的呼叫，但是不能向背景组发起呼叫。 响应组：重要性低于背景组，默认显示在移动终端的组呼列表中。 移动终端可以发起选中响应组呼叫，也可以接收所有响应组的呼叫。 参与组：重要性低于响应组，默认显示在移动终端的组呼列表中。 移动终端只有当组呼选择旋钮切换到当前参与组或选中当前参与组时，移动终端才能对选中参与组发起和接收呼叫。 4、跨系统组呼越区切换：跨系统组呼越区切换是指移动终端在组呼过程中从一个系统基站切换到另一个系统基站的过程，在此过程中通信不中断。 5、跨系统紧急呼叫：跨系统紧急呼叫是指用户在紧急情况下对跨系统固定个号、组号或动态个号发起的跨系统语音呼叫。紧急呼叫的优先级为系统最高优先级，当系统无资源时需拆除低优先级呼叫来建立紧急呼叫，且紧急呼叫建立后不能被打断。 6、跨系统广播呼叫：跨系统广播呼叫是一种特殊的组呼，是面向特定的移动终端用户发起的跨系统通话，只有发起方用户能讲话，其他用户只能接收通话。 7、数据业务（短消息、状态信息）：数据业务是指移动终端向跨系统移动终端、调度台或组发送或接收短消息。短消息最长不超过 23 个字符。短消息包括文本消息和状态消息。 8、卫星定位业务：卫星定位业务是指移动终端利用空口信令上传该移动终端的卫星定位信息过程。系统订阅移动终端的 BD 卫星定位信息，周期上拉移动终端的定位数据，定位数据中携带电量和场强信息。	

		9、旋钮组附着：移动终端的组附着信息，漫游系统将会同步给移动终端的归属系统，包括背景组附着、响应组附着和当前组附着。 10、跨系统截听：跨系统截听是指授权调度台可实时跟踪和截听某个移动终端用户或组的跨系统语音和事件。 11、跨系统强拆：跨系统强拆是指授权调度台强行结束正在进行的跨系统呼叫（包括正在截听的跨系统通话）并强行释放所占的相应资源。 12、跨系统强插：跨系统强插是指在有调度台或授权手持终端参与的跨系统呼叫中，当有移动终端在讲话时，调度台或授权手持终端可以随时强行终止当前的讲话，获取讲话权。 13、跨系统开关机信息订阅：跨系统开关机信息订阅是指终端将开关机的情况上报给归属系统,归属系统通过 ICC 将这些信息上报给订阅系统。 （4）功能要求 通过部署 ICC 实现省省互联互通后，应满足以下 ICC 功能要求： 互联路由、移动性管理、单呼/短消息/状态信息、段队组呼/短消息/状态消息/紧急呼叫/广播呼叫、分级组、话权控制、媒体转发、卫星定位业务订阅、邻站信息通知、越区切换、截听、强拆、强插。 1、互联路由： 1）ICC 可根据个呼号码或者组呼号码，寻址其归属省份 ICC； 2）ICC 可根据个呼号码或者组呼号码，寻址其本省归属地市 MSC。 2、移动性管理： 1）用户归属省 ICC 维护经本 ICC 漫游到其他省 ICC 的用户位置、归属组和组附着信息； 2)用户漫游省 ICC 维护经本 ICC 漫游到本省地市的用户位置、归属组和组附着信息； 3）用户位置、归属组和组附着信息均根据 pSIP（PDT session initiation protocol,PDT 会话初始协议）交互消息动态记录维护，无需静态配置。 3、语音单呼/短消息单呼/状态消息单呼： 1）ICC 处理省外呼叫请求：(1)被叫是本省用户在本省，将单呼/短消息/状态信息业务发送到归属地 MSC；(2)被叫是本省用户在外省，将单呼/短消息/状态信息业务重定向到被叫拜访的 ICC;(3)被叫是外省用户在本省，将单呼/短消息/状态信息业务发送到拜访地 MSC；(4)被叫是外省用户在外省，拒绝请求。 2）ICC 处理地市呼叫请求：(1)被叫是外省用户不在本省，将单呼/短消息/状态信息业务发送被叫归属的 ICC；(2)被叫是省内用户在外省，将单呼/短消息/状态信息业务发送被叫拜访的 ICC;(3)被叫是外省用户在本省，将单呼/短消息/状态信息业务重定向到拜访地 MSC。 4、段队组呼/短消息群发状态消息群发/广播呼叫： 1）ICC 处理省外组消息请求：(1)省内组有组成员在外省：将请求发送给组归属地 MSC 及其它有组成员的 ICC;(2)省外组组成员在本省：将请求发送给组成员登记的 MSC。 2）ICC 处理地市组消息请求：(1)省内组有组成员在外省：将请求发送给组成员登记的省 ICC;(2)省外组组成员在本省：将请求发送给归	

		属地 ICC 及本省其它有组成员的 MSC。 5、分级组： 1）收到本省地市的分级组请求后，呼叫配置的其他省份 ICC； 2）收到其他省份 ICC 的分级组请求后，呼叫配置的本省地市 MSC。 6、话权控制： 1）话权控制，兼容话权控制系统授权和本地预授权的不同控制方式； 2）话权冲突决策原则：单呼，话权决策最终以发起 MSC 为准；段队组组呼，话权决策最终以组归属 MSC 为准；分级组组呼，话权决策最终以发起 MSC 为准。 7、媒体转发： 段队组：组归属 MSC 负责本省的组呼语音转发，非组归属 MSC 的省份由 ICC 转发； 分级组：主叫方源端 MSC 负责本省的组呼语音转发，非源端 MSC 的省份由 ICC 转发。 8、卫星定位业务订阅： 1）ICC 转发卫星定位业务订阅请求； 2）ICC 转发卫星定位数据； 3）ICC 支持部级调度台和有权限的调度台订阅外省终端的定位信息。 9、邻站信息通知： 1）ICC 转发其他 ICC 的组呼业务信道信息给本省的地市 MSC； 2）ICC 转发本省的地市 MSC 的组呼业务信道信息给其他 ICC。 10、越区切换：越区切换请求经由各省 ICC 转发给目标地市 MSC。 11、截听、强拆、强插： 1）ICC 支持部级调度台对全国通话组进行截听、强拆、强插； 2）ICC 支持省级调度台对本省通话组进行跨省截听、强拆、强插，不能对非本省通话组进行跨省截听、强拆、强插。 12、支持不少于 300 路同时读写，每分钟处理事务数据不少于 6000 条，单表记录数不少于 300W 条，支持不少于 300W 条隶属关系组合。 13、加密/解密，可同时支持不低于 3 路的加密/解密语音的处理功能。	
3	ICC 互联网管软件	ICC 网管中心可以查看上海本市 ICC 与其他省 ICC 之间的联网状态、本市 ICC 告警信息。 1）基本功能 1、支持接入全国 ICC 监控监测中心。 2、负责本 ICC 相关的管理、配置及监控监测，具备用户管理、设备管理、性能管理、告警管理、安全管理、权限配置管理功能，以及漫游终端入网监测和漫游终端的通话权限管理功能。 2）功能要求 1、用户管理 移动性管理，包括查询跨省漫游终端（漫游入和漫游出）的信息，主要包括：个呼号、拜访地信息、漫游入/漫游出的时间。 2、设备管理 设备管理包括：ICC 制造厂家信息；ICC 参数配置；ICC 配置文件的存储、对比和恢复。 3、数据管理	1 套

		数据管理包括对跨省呼叫相关信息的记录和统计，含主叫/被叫号码、呼叫发生时间、结束时间等信息，记录时间不少于 365 天。 4、告警管理 告警管理包括对 ICC 运行状态的监控和对告警信息的管理等内容,具体包括： 运行状态监控：ICC 与省内各地市 MSC 的互联状态、ICC 与其他 ICC 的互联状态、链路质量监控； ICC 告警信息的通知、处理、记录、查询、统计。 5、安全管理 为保障系统安全，安全管理应采取以下措施：ICC 配置数据库的备份存储。网管人员的账号管理；日志管理，包括网络运行日志数据的实时存储、网络运行日志数据的统计、网管操作日志数据的实时存储、网管操作日志数据的统计。 6、权限配置管理 为了保证联网后各 MSC 系统的应用安全,避免非常规操作带来的安全隐患，ICC 需要对跨省的截听、强拆、强插业务进行控制： 部级调度台应能对全国通话组进行截听、强拆、强插。 省级调度台应能对本省通话组进行跨省截听、强拆、强插，不能对非本省通话组进行跨省截听、强拆、强插。 7、网管硬件要求 CPU：≥2.5GHz 14C； 内存：≥8GB； 硬盘：≥1*1TB 7200 RPM+1*256GB SSD M.2 网卡：≥ 1 个千兆网卡； 显示器：≥ 21.5 英寸，分辨率≥1920x1080；	
4	ICC 平台冗余软件包	为确保系统可靠性，ICC 跨省互联中心软件须支持主备冗余配置； 当 ICC 系统平台软件、ICC 网管中心时，实现 ICC 服务系统备份。 1、主备设备间对于需要实时保存的动态数据保持实时同步； 2、主备切换引起的业务中断时间少于 30 秒；	1 套

（三）安全管理措施

安全管理措施包括安全边界和 PDT 安全加固系统。

整套安全边界应包括但不限于：防火墙、交换机、语音安全传输控制系统前置机、语音安全传输控制系统后置机和安全隔离网闸。

序号	名称	配置要求	数量
1	防火墙	1.标准 1U 机架式机箱，配备国产处理器。 2.具备 10/100/1000Mbps（电口）≥10 个，COMBO 口≥4 个，2 个接口扩展槽，标配冗余电源。	1 套

		3.整机最大吞吐量≥17Gbps；最大并发连接数≥500 万； 4.IPSEC 隧道数≥400；SSL 用户数≥100； 5.▲具备安全可靠网络信息采集系统，支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，为内网环境提供安全可靠的环境，提供相关界面截图及相关软件著作权登记证书。 6.支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。 7.可基于 IP 地址、网段、用户、时间、VLAN、协议类型等条件设定入侵防御模块的检测事件。一条策略可以同时引用攻击防护、病毒防护、入侵防护、web 防护、威胁情报、口令防护等安全防护模板。 8.支持并开通 WEB 防护功能，支持对 100 个站点制订 Web 应用防护策略。 9.支持自定义 WEB 安全防护事件，可以对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略。 10.支持检测 WEB 攻击事件，包括：命令执行、蠕虫病毒、木马后门、目录遍历、缓存溢出、跨站攻击、SQL 注入、DoS 攻击、安全绕过、请求访问、信息泄漏、漏洞扫描等类型攻击。 11.产品具备安全运维工具，可通过产品页面 ping、Trace、抓包等日常运维操作，实现管理员故障问题的快速定位。	
2	交换机	1.具备 24 个 10/100/1000Base-T 以太网端口和 4 个 100/1000 Base-X SFP 光口，总计 28 个端口，端口结构为非模块化，支持全双工/半双工自适应。 2.支持端口聚合（聚合组端口最大 8 个端口，最多 24 个聚合组）。 3.支持 STP/RSTP/MSTP。 4.支持 IEEE 802.3ad（动态链路聚合）、静态端口聚合。 5.支持 802.1Q（最大 4K 个 VLAN）、支持基于协议的 VLAN、支持基于 MAC 的 VLAN、支持 GUEST VLAN、支持 VLAN 映射、支持 MVRP。 6.支持静态路由。 7.支持 DHCP Relay、支持 DHCP Client、支持 DHCP Snooping。 8.支持 IPv4、IPv6。 9.支持 VLAN ACL。 10.支持 IPv6 静态路由、双协议栈。	1 套
3	语音安全传输控制系统前置机	1.标准 2U 机架式机箱,配备国产处理器,符合国家安全可靠测评要求。 2.每台服务器各具备 100/1000Mbase-TX 以太接口≥2,标配冗余电源。 3.吞吐量≥800Mbps; 4.可以实现控制信令的双向传输，并支持 SIP、RTP、RTCP 等主流媒体协议。 5.提供对硬件资源和日志的异常行为按照自定义触发规则,通过邮件、短信等方式报警，并提供多种报警处置模式，系统报警策略支持自定义 CPU 报警阈值、磁盘健康度报警阈值、内存使用率报警阈值。 6.流量统计可通过折线图、堆叠柱状图、面积图、饼图等方式直观展示。 7.显示在线运行通道数量，在线连接数量，并显示每个国标设备的编号，在线状态，流传输协议，流量及播放时长并对其进行控制。	1 套

		8.系统不同管理员具备不同权限，配置管理员能够管理业务用户及系统参数，安全管理员能够设置安全参数和访问权限，审计管理员能够管理审计日志。 9.▲具备第三方检测机构出具的检测报告，提供扫描件。	
4	语音安全传输控制系统后置机	1.标准 2U 机架式机箱,配备国产处理器,符合国家安全可靠测评要求。 2.每台服务器各具备 100/1000Mbase-TX 以太接口≥2,标配冗余电源。 3.吞吐量≥800Mbps; 4.可以实现控制信令的双向传输，并支持 SIP、RTP、RTCP 等主流媒体协议。 5.提供对硬件资源和日志的异常行为按照自定义触发规则,通过邮件、短信等方式报警，并提供多种报警处置模式，系统报警策略支持自定义 CPU 报警阈值、磁盘健康度报警阈值、内存使用率报警阈值。 6.流量统计可通过折线图、堆叠柱状图、面积图、饼图等方式直观展示。 7.显示在线运行通道数量，在线连接数量，并显示每个国标设备的编号，在线状态，流传输协议，流量及播放时长并对其进行控制。 8.系统不同管理员具备不同权限,配置管理员能够管理业务用户 及系统参数，安全管理员能够设置安全参数和访问权限，审计管理员能够管理审计日志。 9.系统支持在 IPV4 协议和 IPV6 协议环境下的审计功能，能够记录用户操作行为日志及访问视频流的流量，具备日志存储周期回滚功能。 10.▲具备第三方检测机构出具的检测报告，提供扫描件。	1 套
5	安全隔离网闸	1.标准 2U 机架式机箱，配备国产处理器及国产操作系统，符合国家安全可靠测评要求。 2.内外网单元具备 10/100/1000Mbps（电口）≥2，千兆光纤接口≥2，标配冗余电源。 3.数据传输吞吐量≥800Mbps。 4.支持 WEB 方式管理配置，通过内网侧主机统一配置管理；系统业务在内部可信任端配置管理，外网非可信端不存储任何配置信息。 5.系统实时监控系统硬件状态，包括内外网单元的 CPU 使用率，内存使用率，磁盘空间使用率、磁盘健康度、业务 IO 传输速率。 6.系统支持一键体检，检测整机的系统进程运行状态，包括 WEB、协议转发，日志等功能模块状态，以及内部连通状态。 7.文件同步任务支持自定义同步配置，包括发送线程数，积压批次数上下限，线程栈内存大小及方法区内存大小，提供系统截图。 8.▲产品具备安全相关软件，可通过页面上进行 ping、telnet、arp 等日常运维操作，实现管理员故障问题的快速定位，提高工作效率，提供相关软件著作权登记证书。 9.系统支持常见的 TCP、UDP、FTP、TNS 协议的转发功能，可定义出入口 IP 地址，保证数据包的定向传输。 10.系统报警支持本机报警以及邮件报警,定义邮件报警时间段及报警时间间隔。可自定义报警策略，可定义 CPU 使用阈值报警、内存使用率阈值报警，磁盘空间/磁盘健康度阈值报警以及报警间隔时长。	1 套

整套 PDT 安全加固系统包括但不限于：包括防火墙（4口）、防火墙（6 口）、终端安全防护 EDR、入侵检测、漏洞扫描、数据库审计、日志审计。

6	防火墙（4口）	在 PDT 网络边界部署第二代防火墙提供边界隔离和访问控制能力，实现网络边界的安全防护。 1.性能指标：吞吐量：≥8Gbps；每秒新建连接数：≥10 万；最大并发连接数：≥200 万； 2.硬件配置不低于：接口数量：≥8 个千兆电口，≥2 个千兆 SFP 插槽，≥2 个万兆 SFP+插槽；整机提供网络接口扩展槽≥2 个；冗余双电源。 3.按照警用数字集群（PDT）通信系统技术规范系列标准，满足《信息安全技术网络安全等级保护基本要求》的相关规定。 4.支持路由、透明、混合及直连部署模式； 5.支持静态路由、动态路由、策略路由及 ISP 路由； 6.基于传统五元组、用户、应用、内容、时间等多元组一体化访问控制；支持策略冲突检测、策略冗余检测； 7.支持多运营商接入（内置 ISP 路由），支持多种路由均衡算法及路由备份功能；支持 RestfulAPI 接口，能与第三方管理平台对接，实现自动化运维管理； 8.支持每 IP 连接总数限制、所有 IP 连接总数限制、每 IP 新建连接数限制； 9.具有独立的网站应用级入侵防御功能规则库，数量在 1000 条以上；支持自定义规则库； 10.IPSECVPN、SSLVPN、GRE 多种隧道接入技术，支持 DES/3DES/AES 等标准加密算法及 MD5/SHA1 等标准 HASH 算法；	1 套
7	防火墙（6口）	在 PDT 网络边界部署第二代防火墙提供边界隔离和访问控制能力，实现网络边界的安全防护。 1.性能指标：吞吐量：≥8Gbps；每秒新建连接数：≥10 万；最大并发连接数：≥200 万； 2.硬件配置不低于：接口数量：≥8 个千兆电口，≥4 个千兆 SFP 插槽，≥2 个万兆 SFP+插槽；整机提供网络接口扩展槽≥2 个；冗余双电源。 3.按照警用数字集群（PDT）通信系统技术规范系列标准，满足《信息安全技术网络安全等级保护基本要求》的相关规定。 4.支持路由、透明、混合及直连部署模式； 5.支持静态路由、动态路由、策略路由及 ISP 路由； 6.基于传统五元组、用户、应用、内容、时间等多元组一体化访问控制；支持策略冲突检测、策略冗余检测； 7.支持多运营商接入（内置 ISP 路由），支持多种路由均衡算法及路由备份功能；支持 RestfulAPI 接口，能与第三方管理平台对接，实现自动化运维管理； 8.支持每 IP 连接总数限制、所有 IP 连接总数限制、每 IP 新建连接数限制； 9.具有独立的网站应用级入侵防御功能规则库，数量在 1000 条以上；	2 套

		支持自定义规则库； 10.IPSECVPN、SSLVPN、GRE 多种隧道接入技术，支持 DES/3DES/AES 等标准加密算法及 MD5/SHA1 等标准 HASH 算法；	
8	终端安全防护 EDR	在 PDT 应用服务区的应用服务器上部署终端安全软件，提供病毒防护和补丁管理能力，实现应用服务系统的安全防护避免病毒入侵和非法入侵。 1.支持统一管理，适应云架构，提供统一管理平台,统一管理平台应支持在 BC-Linux 上安装,统一管理平台若只能在非 BC-Linux 上安装,应自带正版系统；统一管理平台安装若需数据库，应自带正版数据库软件； 2.单一统一管理平台应支持至少管控 5000 个 Agent； 3.应支持在 IPv6 环境下工作，支持 IPv4/IPv6 双栈模式下工作。 4.支持探测主机上对内端口及对外端口，可采集端口对应的服务及端口协议信息。 5.支持采集主机上的第三方组件信息，可采集第三方组件的版本、运行路径、运行命令行等信息。 6.支持端口安全防护、扫描防护、IP 黑白名单设置、进程行为控制，支持通过对各类攻击事件的采集分析生成攻击趋势图、攻击分布图等图表，直观展现各类攻击事件。 7.支持白名单及黑名单设置，支持黑白名单批量导出及导入；黑名单下可设置记录并拦截、记录不拦截两种模式。 8.Agent 与统一管理平台间信息需满足传输加密；统一管理平台与 Agent 之间需存在相互认证鉴权能力。 9.支持终端数据的实时备份功能，可保存备份数据不低于 30 天。	1 套
9	入侵检测	在 PDT 通信网内关键节点处(节点包括网络边界、接入层、汇聚层等)，对内部外部发起的网络攻击行为进行检测、阻止或限制，并能够对新型的网络攻击行为进行分析，记录攻击源 IP、攻击类型、攻击目标、攻击事件等信息。 1.1U 机架式设备； 2.1 个 CONSOLE 口，2 个 USB 口； 3.板载 6 个 100/1000M 电口，1 组 Bypass;1 个扩展槽； 4.硬盘容量不低于 1T； 5.整机吞吐不低于 2G； 6.支持检测恶意活动，包括恶意 SSL 证书、钓鱼攻击、非法获取权限等； 7.支持检测漏洞后门类攻击，包括漏洞利用、后门攻击、文件包含、缓冲溢出、目录遍历等； 8.支持检测僵木蠕类攻击，包括木马、蠕虫病毒、僵尸网络等； 9.支持日志告警和内存告警配置，当设备达到设置阈值时会进行弹窗警报； 10.针对 PDT 协议支持异常业务请求监控与报警,包括业务在线离线状态监控、设备离线后发包异常监控、超大流量请求监控等； 11.支持对 PDT 协议握手包进行深度解析,通过自定义场景配置异常行为策略，可完成异常自动阻断。	1 套

10	漏洞扫描	在 PDT 专网部署漏洞扫描系统及时进行漏洞发现以及系统补丁及时升级，减少恶意代码侵犯的途径，对信息系统中的关键服务器进行漏洞扫描，发现由于安全管理配置不当、疏忽或操作系统本身存在的漏洞，同时向管理人员给出相应的解决办法及安全建议。 1.1U 机架式设备； 2.1 个 CONSOLE 口，2 个 USB 口； 3.板载 6 个 100/1000M 电口，1 个扩展槽； 4.存储不低于 1T 硬盘； 5.支持系统扫描，最大可扫描 IP 或域名数不少于 1270，扫描任务并发不少于 5，扫描 IP 并发不少于 100； 6.采用 B/S 设计架构，SSL 加密方式通信，无须安装客户端，用户可通过浏览器远程管理系统； 7.能对 PDT 系统专有的业务服务器（如调度中心、网管中心、交换控制中心等）和基站（信道机和基站控制器等）设备进行扫描，可以适配主流品牌厂商的 PDT 设备特点制定对应的扫描策略； 8.支持分布式部署，管理中心统一下发策略、查看任务结果、导出报表，无需登录子引擎；支持从管理中心查看子引擎及其状态；管理中心、子引擎均可执行扫描任务； 9.支持针对已有任务做任务复制，快速生成一个相同任务，支持对复制出来的任务进行再编辑，包括：基本信息、策略、目标范围、调度、扫描参数； 10.支持 SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP 协议的登录扫描；支持批量导入登录信息、批量登录验证；	1 套
11	数据库审计	在 PDT 专网部署数据库审计，提供对数据库访问行为的监控审计，发现异常产生报警并上传审计中心，并生成报表，设置审计策略。 性能需求： 1.1u 机架式设备； 2.6 个集成千兆电口，2 个扩展槽，16G 内存，2TB 硬盘，SSD128G； 3. 峰值入库速度不低于 5500(条/秒)，峰值事务处理能力不低于 9000(条/秒)，日处理不低于 2000 万条，日志数量存储不低于 8 亿条，无限实例数。 4. 将报文通过网络设备镜像到数据安全行为采集探针进行审计支持 vlan 和 vxlan 环境下审计； 5. 支持审计记录完整的语句详情信息，包括：SQL 语句操作内容、SQL 会话起始时间、SQL 会话结束时间、SQL 执行时间、SQL 模板、所属业务系统、源 IP、源端口、目标 IP、目标端口、协议类型、数据库名、数据库用户名、数据库实例名、计算机名、应用程序名、操作方式、操作对象、执行时长、执行结果、错误代码、语句大小、影响行数、绑定变量等至少 24 个项； 6. 支持提取 PDT 系统的个呼号和组呼号信息； 7. 支持设定用户行为异常策略,通过实时监控判定开户的行为与漫游的行为合规性与准确性； 8. 支持双向审计，审计内容包括返回字段、执行结果、影响行数、执行时长、错误代码等，并能够根据执行结果、影响行数、执行时长、	1 套

		错误代码设置审计策略； 9. 支持不同业务系统之间、不同数据库之间、不同访问源 IP 之间在指定时间范围内的对比分析，或同一业务系统、同一数据库、同一访问源 IP 在不同时间范围内的对比分析； 10. 支持数据白名单过滤配置，根据指定 IP 分析、指定 IP 排除、指定端口分析、指定端口排除，减少设备执行数据过滤时的性能消耗。	
12	日志审计	提供对 PDT 全网网络设备、主机、应用系统日志的集中收集、分析、关联、有效的发现安全事件隐患。并对探针系统采集并发送的流量日志信息进行采集、存储、识别、关联分析。 性能要求： 1.1u 机架式设备； 2.硬盘容量不低于 1T； 3.网卡口:6 个 10/100/1000MBase-T 电口,1 个 Console 口,2 扩展槽； 4.不低于 50 个日志源； 5.日志容量不低于 1 亿条； 6.支持市面主流安全设备、网络设备、服务器、操作系统、应用系统、管理平台等设备对象的日志采集； 7.支持主动、被动相结合的数据采集方式；支持日志转发；支持 Syslog、API 进行数据采集； 8.支持多条件组合查询（两个查询条件）下查询性能不低于 5000 万条记录/秒；支持嵌套查询；支持字段值精确查询， 9.支持日志按条件进行过滤，类型包括：资产 IP、来源 IP、来源端口、目的 IP、目的端口、资产类别、事件级别、事件名称、发生时间等；搜索语法有精确搜索和模糊搜索两种形式； 10.支持对自身运行的 CPU、内存和磁盘空间等的使用率设置告警阈值； 11.支持对不同 PDT 系统品牌厂商的日志信息进行解析； 12.结合 PDT 系统告警日志明细，可支持对基站离线相关信息、终端注册失败信息、互联状态异常信息、呼叫异常状态信息进行记录留痕。	1 套

五、进度安排

2026 年 11 月 30 日前完成项目交付。

根据本项目的建设规模、投资规模和建设进度要求，以达到一次规划、一次设计、一次施工的原则。

投标单位需根据本项目的建设周期要求，提供合理的建设进度计划和时间进度表。

六、实施要求和技术服务要求

投标人应针对本项目的具体情况，通过对核心参数指标分析，从材料或配件选择、生产制造工艺、整体产品可实现的各项功能指标、实施过程的质量控制管理、安装调试、售后服务等方面编制技术标。

（一）安装调试

合同签定后，投标人需派有经验的技术人员免费到用户现场进行指导，并根据用户的需要，为用户提供终端的安装与调试服务。

（二）技术服务及培训

投标人应根据用户需要提供技术培训手册，包括设备的操作使用、一般故障排除、简单产品维修等。同时，投标人应按用户要求派有经验的工程师免费提供现场技术培训，使用户能够熟练掌握并独立操作。

（三）售后服务

1）维保服务

投标人需提供完整的售后维保服务方案，包括（但不仅限于）①售后服务本地化机构及人员；②响应时间（提供 7×24 小时电话技术支持等）；③定期安排技术人员针对产品的使用环境、使用频率及更新等进行回访、巡检、维护、保养等。

2）故障处置

中标人应在接到设备故障的通知后，工作时间立即响应，无法远程处理的 1 小时内到现场，2 小时内排除故障。非工作时间 20 分钟内响应，无法远程处理的 2 小时内到现场，4 小时内排除故障。

3）质保期

本项目所提供的所有设备需提供 36 个月原厂免费保修、终身维修服务。

（四）应急保障要求

为确保系统的运行稳定可靠，公安业务的正常开展，投标单位需提供完备的应急保障方案，至少包括：日常运行维护、重大活动保障、故障处理等情况。投标单位需提交类似项目的应急保障案例及用户证明。

本项目的免费保修期不少于 36 个月，硬盘等存储介质在免费保修期内不返还。投标人需提供 7*24 小时售后服务、4 小时响应、2 小时到现场、免费保修期内提供定期巡检等；投标人需明确培训方式、培训人员数量、培训内容等方面要求；项目建成后，中标方应向用户提供完整的技术资料，包括设备随机资料、应用软件源程序及介质、用户手册、管理员手册、安装指南等用户文档资料。

七、招标方案、投标书应答要求

投标人所提供的投标方案需要包含招标文件所提出的所有需求。投标方案技术部分应包含以下部分：

1、项目交付方案（包括总体方案、分项实施方案、项

目实施进度计划等），投标人应对需求中的各项逐一进行说明回应（满足、部分满足（应标明不满足部分）、不满足），如未作回应的视为不满足。

2、投标设备材料情况（包括投标全部产品清单表，投标产品技术规格、偏离表，投标设备、配置明细表等）

3、项目服务质量保证措施(包括安全保密措施、应急处置措施等)

4、投入本项目的人员组成情况（包括《项目人员汇总表》、《项目主要人员基本情况表》）

5、其他需说明的问题或需采取的技术措施。

八、项目验收

（一）设备到货验收

（1）货物到达现场后，由中标人提交到货清单，招标人在中标人和监理单位在场情况下检查外观，作出外观记录，双方签字确认，并与中标人代表共同对货物开箱验收。对到货产品与投标产品不一致的，招标人有权拒绝接收。

（2）中标人应保证货物到达用户所在地完好无损，如有缺漏、损坏，由中标人负责调换、补齐或赔偿。

（3）中标人应提供完备的装箱单和合格证等。

（二）项目初验

项目建设完成后，由中标人提出初验申请，招标人组织对项目进行初验。

（三）项目终验

项目初验合格后，系统试运行 1 个月，由中标人提出终验申请，招标人组织对工程进行终验。

终验合格后，系统所有权交付招标人投入正式运行，开始计算质保期。

九、预算明细

序号	工程名称	单位	数量	预算金额（万元）
1	P-PoC 公专网融合通信系统			
1.1	P-PoC 公专网融合通信系统	套	1	56.15
1.2	网关服务器	套	1	8
2	ICC 互联平台			
2.1	ICC 互联平台服务器	套	2	6
2.2	ICC 互联平台软件（含加密狗）	套	1	124.75
2.3	ICC 互联网管软件	套	1	12
2.4	ICC 平台冗余软件包	套	1	9.51
3	安全产品			
3.1	安全边界			
3.1.1	防火墙	套	1	5
3.1.2	交换机	套	1	1
3.1.3	语音安全传输控制系统前置机	套	1	13.05
3.1.4	语音安全传输控制系统后置机	套	1	13.05
3.1.5	安全隔离网闸	套	1	7
3.2	安全加固设备			
3.2.1	防火墙(4 口)	套	1	7.5
3.2.2	防火墙(6 口)	套	2	23
3.2.3	终端安全防护 EDR	套	1	9.9
3.2.4	入侵检测	套	1	6.4
3.2.5	漏洞扫描	套	1	10.5
3.2.6	数据库审计	套	1	10
3.2.7	日志审计	套	1	9.3
	总计			332.11