采购需求

2-需求公示附件：采购需求

A 包采购需求

海南公安“智慧微警务”项目—基础平台及应用（A）包招标需求书

1 项目概述

1.1 项目背景

根据“便民、惠企、利警”理念，运用移动互联网思维，围绕当前群众广泛关注和亟待解决的民生问题，把简政放权、放管结合、优化服务改革推向纵深的关键环节，以互联网思维创新海南公安领域各业务工作模式，拓宽服务渠道和服务内容，充分发挥信息化在系统整合和资源优化配置中的作用，强化信息共享和服务协同，有效提升公共服务水平，持续改善海南省公安便民惠企的各项服务，深入推进大众创业、万众创新，让群众和企业少跑腿、好办事、不添堵，共享“互联网+政务服务”发展成果。

推动公安打击、防控综合实力的再提升，进一步促进经济社会和谐稳定发展，实现深度连接整合公安便民服务资源，以全民服务、利警服务、开放平台、上下级平台联动、移动警务基础平台等需求为核心，以云计算、大数据、移动互联等先进信息技术为支撑，基于实名认证安全保障，公众可以在任何时间、任何地点通过网站、微信公众号、小程序等方式，体验海南公安提供便民服务，实现智能感知的、主动推送的、个性化的全渠道服务。同时，民警也可以随时随地通过移动警务终端应用进行移动协同办公、移动执法办案、现场业务办理、在线便民服务等工作。以开放平台的方式为各警种、各市县公安机关等部门提供建设和运营支撑，为智慧创新警务管理者、业务建设方提供全面的平台服务与支撑能力，实现持续生态发展，打造海南警务信息智能岛和海南平安岛。

1.2 项目目标

一是真正实现民生警务服务线上“一网通办”（一网），线下“只进一扇门”（一门），现场办理“最多跑一次”（一次）。海南公安“智慧微警务”项目是解决过往审批手续冗杂、证明材料众多的重要举措。本次项目将实现 348 项公安民生服务事项线上办理，极大程度提升民众办事效率和满意度。

二是人工智能应用覆盖便民惠企利警全业务。海南公安“智慧微警务”项目在民众的应用侧，实现小助手“小琼”的快速指引，老百姓应用无障碍；在民警的应用侧，只需要对移动警务终端说话，即可进行模糊查询；治安民警在盘问时可用移动警务终端对着嫌疑人，即可自动在“云搜”上搜索，实现“以图识人”；

在马路上遇到可疑车辆，拍个照片即可“以图识车”；社区民警拍个门牌照片即可“以图识户”，从而知道房屋住着什么人等。本次项目实现 17 项移动警务应用上线，预计将提升民警 30%及以上的工作效率，为民警的工作和生活带来良好应用。

三是实现“组织活跃、扁平管理、高效运作”的目标。各层级、各部门可通过“同事圈”分享动态、好文、知识，各工作组可按需建群、即时沟通，让差旅途中的民警也能随时加入讨论中，“投票”、“评论”等功能让民警以主人翁姿态参与单位事务管理，可集众智参与社会治理，让领导的理念和意图通达基层民警，防止信息“失真”、“变馊”，也让基层民警的意见建议直接通达上级领导，形成更加民主的氛围，激发全体民警的主人翁意识和参与管理的热情。

四是全面整合信息资源，把好信息采集“入口”，对重复采集录入采取“零容忍”，让民警减负。过去几年来，公安信息化的迅猛发展，从部、省、市推广应用的信息系统众多，在电脑端形成了“烟囱林立”和“信息孤岛”问题，在移动警务这个新的重要平台上，不能让同样的问题再次发生。通过警务终端，民警在手机上对同一数据“只录入一次”，实现“核验即采集”，避免专门采集、多次采集、低效采集，实现“一次采集、全网共享”。

该项目的建成将给海南省人民群众的生产、生活带来极大方便；同时通过信息化技术和数据共享，大幅减少广大一线民警的工作量，有效提升公安一线的警务效能，极大地解放基层公安警力。通过审批服务全流程网上办理，所有收费实现网上支付，民警不直接接触所收钱款，从机制上有效杜绝了“吃拿卡要”等群众身边的腐败问题，有利于促进公安队伍作风转变，树立公安机关良好形象。

按照“统一接入、集约建设“原则，明确海南智慧微警务项目建设包括省级及地市，其他地市、警种不单独规划。

1.3 总体建设内容

海南公安“智慧微警务”项目的主要建设任务如下：

1、搭建海南公安“智慧微警务”项目基础运行环境：包括移动互联网服务子平台、联网服务子平台、移动安全接入子平台、公安信息网服务子平台。

2、建设海南公安“智慧微警务”项目安全体系：包括移动互联网服务子平台安全内容、联网服务子平台安全内容、移动安全接入子平台安全内容、公安信息网服务子平台安全内容、移动警务 PKI 安全接入平台升级及应用改造、移动终

端安全。

3、建设海南公安“智慧微警务”项目应用支撑平台：为全省公安机关便民惠企服务、利警服务的移动化提供统一的应用支撑平台。搭建移动应用超市，实现移动应用的发布、审核、上架、下线等管理。可以把海南公安“智慧微警务”项目应用支撑平台看作是“航母平台”，厅机关、各警种、地市公安在这个平台上共享基本功能、通用功能，并可以根据需要开发自己的专业功能，形成一个共建、共享、共用的移动警务应用生态圈。并实现 3 家运营商网络同时接入及实现通过公安部检测的多种安全监控组件同时接入并管理。

4、建设海南公安“智慧微警务”项目便民惠企服务应用：建立全省公安互联网+政务服务系统，包括微信公众号、小程序、网上办事大厅等，实现统一门户和身份验证，建设包括交警、出入境、户政、治安、监管等便民惠企应用。

5、建设海南公安“智慧微警务”项目利警服务应用：建立统一的“警务即时通信”平台，支持互联网、移动信息专网和公安网的 PC 端和移动端。“警务即时通信”平台包括即时通信、移动警务应用的统一入口，实现统一的用户身份认证、消息推送等服务。建设一批日常应用和警务应用，日常应用包括移动 OA、通知公告、会务助手、督办、访客系统、动态（朋友圈）等应用，警务应用包括云搜、社区警务、户政、治安、出入境、交管、情报等应用。按照公安部对移动警务即时通信工具的互通协议标准规范，实现与公安部及各省公安厅即时通讯系统的互联互通。

2　项目建设需求

本项目的建设主要包括便民惠企服务和利警务服务的应用。

2.1 便民惠企应用技术需求

便民惠企应用是面向千万民众级别使用的业务应用，主要包括户政、交通、出入境等业务服务，比如户口申报、户口迁入、驾驶证业务、交通违法处理、普通护照首次申请、往来香港个人游签注等。

2.1.1　功能要求

各业务由民生服务开放平台进行全流程管理，提供标准的业务模板库，包括流程模本、页面模板、业务数组库等，同时提供标准的 UI 组件和丰富的视觉设计资源构建开放生态；整合公共支撑平台，提供应用支撑能力。

同时，开放平台提供小程序的快速发布，生成工具和开发管理；包括可视化页面关系管理，可视化页面封装，可视化页面数据编辑，一键生成小程序；基于开放能力、开发资源库，分工分步合作，流水线式小程序开发，通过可视化开发平台快速交付民生小程序。

建立全省公安互联网+政务服务系统，包括微信公众号、小程序、网上办事大厅等，实现统一门户和身份验证，建设包括交警、出入境、户政、治安、信访等便民惠企应用。

“海南警民通”便民惠企服务应用将主要在海南省政府公安厅门户下面设立二级栏目作为应用入口，配合“海南警方”公众号进行推广。

2.1.2　业务需求

根据国务院办公厅印发的《国务院办公厅关于印发进一步深化“互联网+政务服务”推进政务服务“一网、一门、一次”改革实施方案的通知》（国办发〔2018〕45 号）文件精神，结合海南省的实际情况，便民惠企服务需求主要在以下几方面：

1、户政（治安）业务功能：包括户口申报、户口迁入、户口迁出、市县内迁移、户口注销、立分户、证件办理、便民查询等功能。

2、治安业务功能：包括娱乐场所登记备案、管制器具备案、危险化学品备案、民用爆炸品备案等相关业务功能。

3、交管业务功能：包括驾驶证业务、交通违法处理、机动车业务、预选车牌、考试预约、事故快处、通行证办理移机交通违法异议申诉受理等业务功能。

4、出入境业务功能：包括证照网约先办、便民服务查询、线上业务办结、线下服务预约、综合业务办理、企业服务预约以及政务信息公开等业务功能。

5、综合警种业务功能：包括监管、宣传、禁毒、网安等警种业务的在线办理和操作指南等业务功能。

业务分类	跑 1 次	跑 0 次
一、治安业务	41 项	17 项
二、户政业务	137 项	0 项
三、交管业务	33 项	17 项
四、出入境业务	73 项	2 项
五、网警业务	3 项	0 项
六、监管业务	1 项	0 项
七、边防业务	10 项	0 项
八、法制业务	0 项	10 项
九、咨询建议业务	0 项	4 项

2.1.3其他需求

1、微信小程序需求：实现公安系统内各类业务办理无缝对接，公安各系统业务办理全覆盖。社会公众在门户网站可以进行各警种业务办理或预约，了解公共安全、警务活动宣传等警民互动。

2、数据统计分析系统需求：根据社会公众办理的业务数据进行多维度全方位统计，实时绘制报表进行可视化数据分析展示。

3、统一业务预约系统需求：在业务办理平台中进行每天业务预约人数设置，控制每天大厅业务办理量，提升公安预约办理服务能力。

4、咨询建议系统需求：根据社会公众用户反馈的咨询建议信息进行一对一高效化服务，提升公安便民服务能力。

5、智能审批系统需求：包括户政、治安、出入境、交巡警等各警种业务数据展示、审批、各地市业务审批权限划分等。提供扫描上传功能，产生证照的业务事项可提供邮寄选择服务，物流信息实时追踪。全面深化全流程网上办理深度，

实现申办材料的“无纸化”流转。

6、PC 系统需求：实现小程序与 PC 端统一用户管理和单点登录功能，与公安系统内各类业务办理无缝对接，公安各系统业务办理全覆盖。社会公众在门户网站可以进行各警种业务办理或预约，了解公共安全、警务活动宣传等警民互动。

2.2 利警应用技术需求

本期项目建设主要包括 700 余人省厅机关用户的移动警务使用，实现省厅 17 项功能应用，同时在本期项目中能够支撑移动警务平台基础资源需求。项目建成后，省厅机关的第一批警务应用将在移动警务完成，如即时通讯、移动办公、机关服务、专业应用等，后续将规划、建设、迁移更多警种和欠发达地市民警的移动警务应用。

本方案在架构上是按完整支撑全省 13000 民警以及 7000 辅警的使用来进行设计。

即时通讯（警务微信）：似于“微信”的即时通信工具，主要解决省厅内部的即时沟通、移动办公、一体化集成化办公的问题。

日常应用：构建沟通，协同，社交于一体的海南省公安智慧微警务平台，包括：移动 OA、动态（朋友圈）、厅长点评推送、通知公告、会议助手、新闻推送、业务看板、维修报障、督办、要情速递等 10 个应用。

专业应用：包括云搜、云回答、社区警务、党建、情报、指挥等警务应用。

2.2.1即时通讯（警务微信）

全省公安机关警务、基层警务提供统一的即时通讯平台，与“微信”等即时通讯软件使用体验接近，并同时支持互联网、移动信息网和公安网的 PC 端和移动端，作为海南公安“智慧微警务”项目的统一入口，提供统一的用户身份认证、消息推送等服务。未来将按照公安部对海南公安“智慧微警务”项目即时通信工具的互通协议标准规范，打通与公安部、本省使用即时通信产品的地市。需要与海南省公安厅现有公安信息网即时通讯工具（警务微信）进行对接，提供对接方案实现及现有即时通讯消息互传。

治安防控长效机制中社区治安维护需要发动多方协同，为支持群防群治工作，警务微信需要具备和互联网主流社交平台实现消息透传能力。

高度安全的私有化部署：警务微信需要私有化的部署在部门网络环境下，遵

循现有的各类安全体系要求。

高强度的数据加密：在沟通数据的网络传输、服务端存储、终端存储需采用高强度的加密算法和密钥，避免内部沟通数据被破解。

高度复杂的网络安全支持：需支持各类复杂的网络安全规范要求，需支持穿透各类安全设备，包括防火墙、网闸、光闸等。

即时通讯软件需支持超大规模的用户量,用户体验设计都沿用主流即时通讯软件的设计思路，界面风格、操作方法和微信等主流即时通讯基本保持一致，使用户的学习门槛低、易上手。

作为时沟通的工具，与其他应用功能配合使用打造完整的办公协作生态体系：

利用服务号、小程序等应用，触达微信 C 端个体用户，构建起完整的用户服务体系。

为了打造“一体化、系统化、发展性”的信息化建设整体方案，警务微信需提供定制开发能力，客户可以基于这些能力对其进行扩展，实现与内部的各种信息化平台的整合对接与创新服务模式的探索：

提供丰富的信息沟通渠道：需提供 SDK 供各类应用系统进行整合，使这些应用系统具备丰富的信息沟通渠道，随时在应用系统中发起各种消息通知、一对一沟通、群组沟通。

提供边界应用集成入口：需要提供在工作区域和沟通窗口中发起各类应用的调用入口，在沟通过程中随时推进各类工作的完成，并反馈最新的工作进展。

即时通讯作为移动警务系统的核心平台，作为警员最高频使用的移动端平台，需要为各类警务应用提供相关的应用支撑能力：

1、即时通讯能力：提供各种消息类型的发送、接收和处理，可以根据业务需要，在应用中整合即时通讯的能力；支持互联网、移动信息网和公安网三网消息互联,例如公安民警可以将互联网的公众微信朋友圈的文章点评后转发到移动信息网的警务微信的同事圈中。

2、群组沟通能力：提供对群组沟通的能力，可以根据业务需要，在应用中整合群组沟通的能力；提供二次开发的平台能力，可以在群组中根据业务场景整合任务、督办、问询等功能，群组中所有讨论记录和文件都自动放在云盘，并详细记录时间。

3、组织架构管理能力：提供对组织架构/通讯录进行管理，实现组织架构和用户的同步。

4、前端应用开发 JS-SDK：提供完善的 JS-SDK，帮助各类警务应用集成即时通讯平台的前端能力，包括对文件、图片、音频等的处理。

5、警务应用管理：提供面向警务应用的接入管理，实现警务应用的统一入口和统一身份验证。

关键功能点：

1、消息管理中需要支持：移动端支持通过摄像头扫描纸质文件并生成 PDF 格式发送给联系人。消息在手机端设置定时提醒。

2、勿扰模式 开启休息一下，休息期间不再收到任何普通消息提醒，重要联系人的消息依然会提醒。

3、扫码入口支持扫描条形码。

4、手势密码、面容识别与指纹识别 政务微信移动端支持手势密码、面容识别与指纹识别，帐号登录后，再次打开客户端时，需要验证通过后才能使用政务微信。

5、限定成员可修改字段 管理员可根据现实需求设定机构成员可以自行修改哪些个人资料，如：手机、头像、邮箱、姓名等。客户端登录限制 支持限制成员登录某个客户端。

6、通讯录管理设置 管理员可在后台设置隐藏组织节点或成员，被隐藏的部门或成员，不会显示在通讯录中，方便对于重要或机密的部门人员进行有效保护。

7、第三方加密（国密） 国密 采用支持国密标准的第三方加密服务，实现对敏感信息的二次加密，，支持 SM-2，SM-3，SM-4。消息传输和存储全程采用国密算法加密，保证信息安全。移动安全管理 管理员可以禁止移动端的图片或视频保存到手机，防止重要信息外露。

8、聊天内容跨网络脱敏控制，可以精确设定以下内容跨网络是否脱敏显示，包括但不限于：文本消息、表情、图片、文件、位置、语音、视频、会议、红包、聊天记录和应用消息。

9、外部组织间的信息互通 不同外部组织架构间的互联互通 支持不同省市外部组织间的互联，例如一个省可以添加另一个省公安的用户为好友，可以加入单聊或群聊。

2.2.2日常应用

2.2.2.1 移动OA

通过对现有OA集成到警务微信，用户能够很便捷地或自动为便民惠企平台提供数据的支撑通过警务微信平台进行日常办公、查看和处理公文文件、及时接收系统的推送信息、方便快捷的进行流程管理和审批工作。

公文信息推送

通过调用海南公安“智慧微警务”项目平台警务微信的消息推送接口，实现移动端和PC端的公文待办信息推送。

当PC端OA系统或移动OA有最新的待办公文提醒时，系统后台服务将待办公文提醒消息通过消息推送接口对接到警务微信之中。

移动端信息推送功能是对移动办公处理或产生的信息提醒方式进行开发，通过调用警务微信消息推送的接口，实现将移动办公过程中新产生的待办公文、用户关注的公文进行消息推送到警务微信，用户可以通过警务微信消息界面中直接打开某条消息进行查看和批示该公文。

移动OA信息推送功能需要在移动OA的WEB服务中部署信息推送的后台服务，后台服务自动将移动OA产生的待办提醒信息对接到警务微信消息端之中。

移动办公界面WEUI化设计

为实现移动OA与警务微信统一界面风格，移动办公系统将基于WE UI 的规范进行界面设计、开发。界面设计内容包括：界面风格和页面风格。

1、界面风格

移动OA应用警务微信WEUI风格，对移动OA的主界面、各二级目录列表页面等应用，从表单、基础组件、操作反馈、导航相关、搜索相关、层级规范等方面进行利用设计，并实现主界面支持列表、九宫格显示，系统管理员可以根据系统风格要求进行自行设置移动OA的整体风格界面。

2、页面风格

移动办公各功能页面应用警务微信WEUI风格，对移动OA的公文处理表单、信息显示页面、会话窗口等信息页面，从表单、基础组件、操作反馈、导航相关、搜索相关、层级规范等方面进行利用设计，调动相关样式和图标，保证与警务微

信风格一致。

移动界面功能

移动界面主要是为登录移动 OA 的用户提供快速查找相关功能的列表显示界面，移动 OA 应用提供手机端发文、收文功能。

发文处理功能

移动 OA 应用发文处理包括一是启动发文流程进行发起公文拟稿审批，二是各步骤经办人员进行对发文进行审核、会签、签发、正文修订批示等两方面处理过程。

操作和流转过程与厅现有办公自动化系统一致，并实时同步更新，相关处理过程的功能和操作方式在以下的界面功能和审批处理功能中进行描述。

收文处理功能

移动OA应用收文处理与发文功能类似,移动OA应用的收文处理有两种方式：一是收文人员收到纸质来文材料，二是通过公文交换系统对接到厅 OA 系统的自动来文。

对于纸质来文，可以由收文人员在移动 OA 中发起收文流程，填写收文表单的相关信息，将纸质材料通过拍照上传的方式将材料上传到流程的附件中，进行发起拟稿审批，各步骤经办人员根据来文内容进行收文批示、主办协办处理、处理结果反馈、办结等处理过程。

对于自动来文，公文交换系统会将各单位来文信息、附件材料对接到收文人员的待办列表中，收文人员根据来文性质提交到各步骤经办人员进行收文批示、主办协办处理、处理结果反馈、办结等处理过程。

操作和流转过程与厅现有办公自动化系统一致，并实时同步更新，相关处理过程的功能和操作方式在以下的界面功能和审批处理功能中进行描述。

界面显示的功能主要分为常用公文、常用事务、其他功能三大类，其中常用公文包括：待办公文、待阅公文、内部交流、已办公文、已阅公文、所有审批、公文查询等；常用事务包括：请休假申请、车辆申请、会议室申请等；其他功能：日程安排、OA 问题反馈、个人设置等。

移动审批处理功能

移动审批处理主要是实现用户在移动 OA 中进行启查看表单、查看正文和附件等信息,并可对表单进行填写审批或办理意见、支持正文和附件的预览及编辑、

公文的审批发送或意见保存等操作。

移动扩展应用

移动扩展应用是在现有 OA 系统延伸的移动审批功能基础上，从办公用户移动办公实际需求出发。融合“互联网+”创新思维，扩展关注公文、收藏公文、@某人提醒等功能，让移动办公在保留原有的规范流程基础上，可以让用户自行管理与本职相关的各种公文或事务。

后台管理

后台管理为移动 OA 通过 PC 端进行后台配置信息的管理的功能，包括对日志管理、推送消息查询等功能。

2.2.2.2 动态朋友圈

应用以互联网社交和自媒体思维为基础，着力打造海南公安“智慧微警务”项目中全体公安干警均能参与的集互动、便利、自由、趣味于一体的全新办公生活体验型应用。

“动态朋友圈”由全部动态，关注，精华，热门话题，动态查询，个人主页，个人设置，后台管理等模块组成，模块间分别显示，内容相通。

“动态朋友圈”以发动态、参与话题讨论、精华动态，厅长点评为主要功能，内部互联互通。

2.2.2.3 厅长点评

“厅长点评”着力为全厅打造一个实时了解领导最新指示的平台，让全厅可以围绕重点问题与话题展开有益的充分的讨论。

“厅长点评”突出的展现厅长对于某个动态的点评内容，并可以全厅推送，让全厅可以第一时间学习、领会领导批示。

包含厅长点评、消息推送、点评列表三个功能模块。

“厅长点评”主要围绕的是厅长的“点赞”、“评论”、“发表动态”来进行消息的推送。

2.2.2.4 通知公告

依托省海南省公安智慧微警务平台，新建一个通知公告移动应用，既可以从 PC 端发送图文通知，也支持通过移动端发送图文通知。通知送达后有消息提醒，防止接收人员遗漏。

通知发送人可以方便地选择通知发送覆盖人员范围。通知发送人通过应用可以清晰了解哪些人已经阅读了通知哪些人尚未阅读。

2.2.2.5 会务助手

依托省海南公安“智慧微警务”项目平台，新建一个会务助手移动应用，通过移动端的会议管理系统实现快速建会、会务通知快速下达、在线报名参会、会议变更及时通知到位、参会人员请假方便、发送参会提醒等实务功能，大幅度提高会议管理力度，提高办会效率。

会议通知发起人在线发起会议，由会议通知接收人线下与领导确认参会人员后，在线提交参会名单，并发通知给发起人与参会人员；参会人员收到会议通知，若因事无法参与线下告知，会议通知接收人线上为参与人请假，并发通知给会议发起人。

2.2.2.6 督办

依托省公安厅海南公安“智慧微警务”项目平台，新建一个督办工作移动应用，将督办工作从完全线下的方式转变为线下线上相结合的模式。该应用除了为省厅的督办工作提供支持外，还可以给各级有督办事务需求的单位提供支持。通过该应用达到督办任务相关人员随时可达、督办任务详细资料随时可查，全面实现“在线”督办。

在领导作出批示以后，由督办科人员发起督办，线上填写审核人、签发人，一次性指定一级经办人员并填写交办意见；一级经办人收到经办消息提醒，点击可进入督办详情页，需要时根据批次添加经办意见； N 级经办人（N>1）收到经办消息提醒，点击进入督办详情页，需要时分批次添加经办意见，并线下反馈给一级经办人；一级经办人线下汇总所有经办情况后，线上统一申请办结；督办科人员收到每个一级经办申请办结提醒并处理，填写整个督办事项跟进状态（既修改督办状态：已交办、如期推进、逾期、严重逾期、已办结），若判定状态为已办结，则一级及下级经办人收到督办事项已办结消息提醒，完成督办事项。

2.2.2.7 维修报障

实现省公安厅移动办公智能化，及时性、准确性、全面性解决厅内各设备故障问题，保证警务工作顺畅，提高后勤业务效率和业务水平。

维修报障系统包括 PC 端、即时通讯软件等展现形式。其中 PC 端包括维修人

员管理、领导人员管理、报障申报办理等功能模块。即时通讯软件包括查看处理汇总情况、维修报障清单、水电报障、空调报障、电梯报障等功能模块。

2.2.2.8 要情速递

依托省海南公安“智慧微警务”项目平台，新建一个要情速递移动应用，实现重要事项的快速传递，做到传递路径可查，送达结果可查，可自动或者手动对相关人等发送未阅提醒，确保重要消息送达目标。

速递发起人：输入简单标题和内容，选择接收人后新建速递。可以对接收人进行未阅提醒并查看整个速递的转发明细。

接收人：收到速递通知，并查看速递。查看后可以选择结束或转发，如果转发需要输入转发批注并选择转发接收人。可以对转发接收人进行未阅提醒，并查看自己下线的速递转发明细。

转发接收人：收到速递通知，可以查看速递发起人填写的内容和速递流转到自己手中的整个流转痕迹及每一次转发的批注。

2.2.2.9 新闻推送

根据警务微信平台的接口标准规范，对现有新闻管理系统进行升级改造，提供手机版新闻推送功能，用户可以及时了解新闻内容。

2.2.2.10 业务看板

依托省海南公安“智慧微警务”项目平台，建设统一数据统计分析平台，以业务办理量、业务办结量等相关智能分析看板。让各省、市、县公安掌握各地业务办理数据统计分析。

海南省公安通过统计分析看板对所有的业务办理情况和业务办理量、公众关注热点等情况进行相应的统计和分析。

2.2.3 专业应用

2.2.3.1 云回答

“云回答”应用以互联网思维为指导思想，尽力为用户打造一个可以对知识进行沉淀的互动平台，能够真正为用户提供具有实际价值的“问答”服务。

云回答首页包含搜索、排行榜、待答、全部问题、我的（包含关注、提问、回答、收藏）共五个主要功能模块。

“云回答”服务的主要流程是：搜索、提问、回答、采纳以及积分的计算和

排行。流程尽量的清晰简单，让用户将注意力集中在问题和回答本身。

2.2.3.2 党建

党建系统旨在依托现有资源，充分了利用移动互联网平台，创新基层党建工作方式，增强党建工作活力，推进基层党建工作信息化建设，为基层党组织和党员干部群众提供便捷、高效服务。系统的目标是实现党建的信息化、网络化的线上建设，与线下的思想建设、组织建设、作风建设等党建工作与活动保持同步，提高党建的科学化水平。

2.2.3.3 社区警务

在海南公安“智慧微警务”项目框架下，以服务一线民警为宗旨，主要面向派出所一线执行社区管理的民警，能够实现基本信息的查询和业务的自动化处理，建设指尖社区警务应用。

社区警务系统与警务平台和人口管理等系统紧密集成，在完成信息查询的同时可以随时进行其他关联数据库比对信息，实现数据复用、自动比对报警。社区民警信息采集和业务处理系统可以为民警执法提供最大程度的支持，对于摸清管片内治安情况，实现社区管理新模式，维护社会稳定有很大的帮助作用。

2.2.3.4 情报应用

在海南公安“智慧微警务”项目框架下，以服务一线民警为宗旨，从日常民警工作为切入口，建设情报移动应用-指尖情报 APP 系统。让民警可在移动终端实现对情报资源的充分利用。

2.2.3.5 指挥应用

基于移动互联网、公安移动信息网、公安信息网，遵照公安部海南公安“智慧微警务”项目建设指导，遵循公安部海南公安“智慧微警务”项目应用安全接入规范，充分利用省厅指挥四中心建设成果及资源，建设面向指挥业务指挥海南公安“智慧微警务”项目应用-指挥，满足联勤协作、预警处置、现场核实和业务办理等移动化业务需求。方便一线民警通过移动终端完成警情的处置反馈，实现处警过程中的业务联通，实现指令精确下达、情报精准推送、处置及时反馈。

2.2.3.6 云搜（综合查询）

为紧急和突发事件的处理提供信息依据，为突发案件的迅速侦破创造信息条件，通过警务微信终端，实现人脸识别登录，提供进行人员档案、车辆档案以及

人像比对功能，满足民警盘查时对人员车辆核查的需要，实现移动办案、移动侦查、移动监控，是实战运用的新助手。

2.3 应用支撑平台技术需求

海南公安“智慧微警务”项目应用支撑能力建设的最终目标是为公众、省厅/市局及警种管理者、民生警务应用开发者三类角色提供一站式、开放式的全方位服务能力，构建形成“省厅搭台、警种唱戏”的良性生态。因此针对不同的服务对象，需要提供系统化的服务能力建设。

应用支撑平台需要为各类政务信息化应用提供功能完整、性能优良、可靠性高的技术公共组件，解决应用系统建设中的共性问题，为大量具有共性业务需求的政务系统提供完整、健壮的基础支撑能力。开放能力聚合公共支撑平台、云、微信开放平台、警务微信开放平台等基础支撑能力和互联网创新服务能力，通过开放平台智能网关统一提供安全、可控、高效的能力接入。

应用管理为解决构建“互联网+政务服务”集约化建设参与开发商多，开发协同效率低，开发过程缺乏有效管理问题。提供全流程的服务管理，包括开发商管理、项目管理、任务管理、发布管理等全流程开发管理能力。

运营数据平台定位为提供标准的数据采集规范，通过可视化数据后台提供产品流量数据、业务数据一站式查询；基于用户数据、数据来源、数据趋势，对产品成长指标及优化提供依据；通过数据运营管理实现各部门间数据共享，打破信息孤岛；通过大数据分析为精准运营提供数据支撑。

运营管理平台定位为从政务互联网思维角度出发，使运营方式系统化、模块化，将政务产品打造成“群众爱用、亲民有温度”的政府品牌。运营管理平台核心能力涵盖数据运营、用户运营、内容运营、活动运营、事件运营、运营推广等相互支撑构建一体化的运营体系。

2.3.1 总体架构

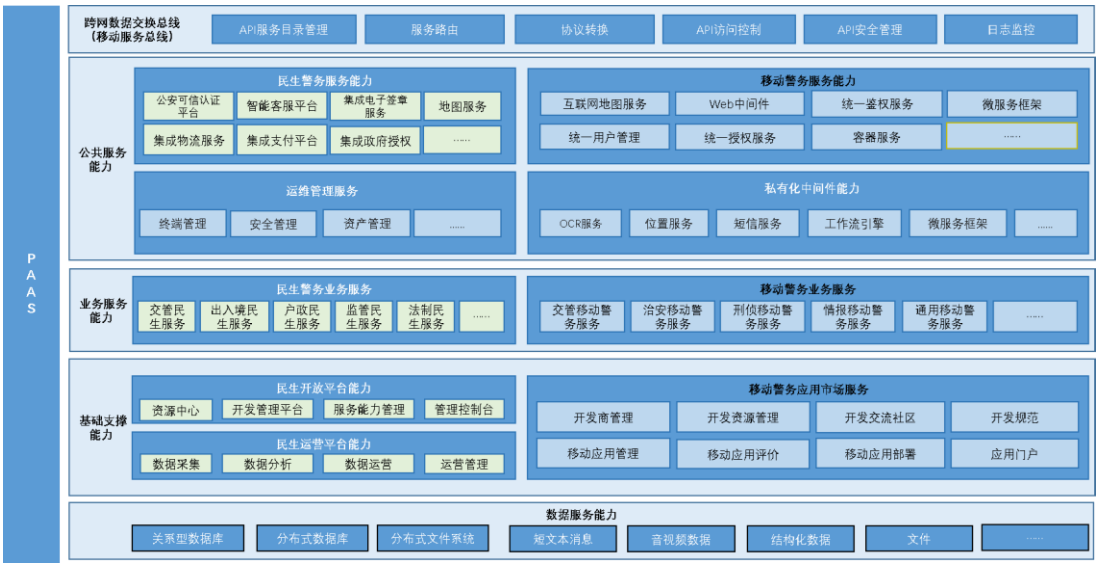

图 5- 1 海南公安“智慧微警务”项目应用支撑平台架构图

如上图所示，海南公安“智慧微警务”项目的应用支撑平台主要包括如下内容：

1、数据服务层包括关系型数据库、分布式数据库、分布式文件系统等；

2、业务能力支撑包括公安可信认证平台、智能客服平台、支付平台、OCR服务、电子签章服务、物流服务、位置地图服务等；

3、开放平台能力包括资源中心、开发管理平台、服务能力管理、管理控制台；

4、运营平台能力包括数据采集、数据分析、数据运营、运营管理；

5、移动警务应用管理包括开发商管理、开发资源管理、开发交流社区、开发规范等，用于支撑移动警务应用的开发、上架、下架等管理。

6、跨网数据交换平台(移动服务总线)主要包括应用网关、API 网关、服务总线、日志监控等，用于支撑应用数据的跨网交换。

支撑层按移动警务规范要求并结合海南实际业务需求进行规划设计。支持多数据服务能力，重复兼任主流数据结构及大数据数据访问。支撑业务类型和对应的数据流转范围分别整合成移动警务及民生警务能力。移动警务部分主要参考移动警务建设标准，整合联网服务子平台、公安信息网服务子平台对民警、辅警软件模块提供支撑。在移动警务中针对移动互联网服务子平台，对外集成服务、地

图、可信认证等整合成民生警务服务能力。私有化中间件等通用功能分别封装可以独立扩展升级。

应用支撑平台及警务应用建设功能需要依据“全国公安移动警务建设总体技术方案（2016 版）”中相关技术标准及功能要求进行规划，重点功能如：“数据交换平台、移动管理支撑平台、可信认证等”标准中明确的功能需要在本次建设中全面支持。

2.3.2统一民生服务开放平台

一级分类	二级分类	三级分类	功能特性
政务开放平台门户	资源中心	接入指南	为政务服务开发者提供快速接入政务开放平台指南，了解如何使用能力、搭建应用。
		小程序资源	▲为政务服务开发者提供如何搭建小程序基础框架教程，节省前端开发时间。包括小程序的开发框架指南、组件工具库、脚手架、设计资源。
		web 站点资源	为政务服务开发者提供 web 政务场景化组件，实现快速开发。包括 web 站点的组件工具库、前端编译工具使用指南。
		H5 页面资源	为政务服务开发者提供政务场景模板，实现快速开发。包括 H5 页面的组件工具库。
	开放能力	文件服务	对接主流云厂商的对象存储服务。
		消息服务	对接邮件、短信、城市服务模板消息推送服务。
		意见反馈	对接用户意见反馈的信息收集、统计、反馈回复等服务。
		人脸核身	对接微信人脸核心，依托生物识别技术，通过人脸识别+公安比对，校验用户实名信息和本人操作。
		支付实名认证	对接微信支付实名认证，基于支付实名用

一级分类	二级分类	三级分类	功能特性
			户基础，提供实名支付账户信息授权接口。
		非税支付	对接微信非税支付，建立并简化各业务部门与财政、银行间非税支付的连接。
		位置服务	对接腾讯位置服务，基于海量位置数据，为客户提供定位、地图、搜索、路线规划、导航、大数据等专业的 LBS 能力支持。
		物流服务	对接主流物流平台，实现办事“不跑腿”，寄件“免填单”，收件“不着急”，办事无忧。
		智能客服	对接智能化客服机器人服务，支持对接后端数据库数据，提供 AI 级人机对话能力，可根据数据库数据及前端输入训练，提高回答的准确性。
		智能文字识别	对接腾讯云 OCR，将图片上的文字内容，智能识别成为可编辑的文本。支持身份证、名片等卡证类和票据类的印刷体识别，也支持运单等手写体识别，支持提供定制化服务，可以有效地代替人工录入信息。
		智能搜索	对接智能搜索服务，提供全文搜索能力，同时提供后端数据接入及前端搜索服务支撑能力接口服务。
	用户管理		为开发商提供项目成员管理的能力。开发商可以对用户进行增、改、查等操作，可为不同的用户指定不同的角色，通过基于角色的权限控制体系实现用户权限控制。
	分项目控制台	分项目概况	开发商登录后，显示需要开发的应用情况、项目成员、开放能力、使用流程等信息。

一级分类	二级分类	三级分类	功能特性
		后台应用管理	开发商可创建后台应用后，在具体应用中进行自己服务的发布创建和申请第三方服务的申请，由经机构管理员在【政务开放平台管理后台——申请审核管理】进行审核通过后，则可调用接口及服务进行开发和部署。
		小程序开发管理	针对机构管理员在【政务开放平台管理后台——小程序开发管理】创建好的小程序模块和代码仓库，开发商可以在代码仓库进行小程序的应用模块开发，以及小程序的多模块在线合包和预览的功能，将不同的模块功能合并成一个独立的小程序并生成开发二维码，开发者可通过扫描二维码测试。
		开放能力申请	提供能力申请和能力申请记录功能，开发商申请的开放能力由机构管理员在【政务开放平台管理后台——申请审核管理】审核通过后开发商即可通过接入指南快速接入使用开放能力。
		IT 资源申请	为开发商提供 IT 资源申请，包括服务器、网络及信息安全资源申请、远程接入申请运维审计申请、业务端口申请、负载均衡资源申请、对象存储申请等，经机构管理员在【政务开放平台管理后台——IT 资源申请审核】进行审核通过后，则可使用相关 IT 资源。
政务开放平	管理控制	全局概况	展示政务开放平台全局的概况信息，包括

一级分类	二级分类	三级分类	功能特性
台管理后台	台		机构与供应商应用指南、系统与应用模块的框架信息等。
		机构管理	为平台管理员提供政府机构信息的管理能力，支持对政府机构进行增、删、改、查以及搜索等各类操作。
		机构成员管理	平台管理员（或机构管理员）可对指定政府机构进行机构成员的管理维护，包括对机构成员的查看、新增、编辑、删除。
		开发商管理	为机构管理员提供开发商信息的管理能力，支持对开发商进行增、删、改、查以及搜索等各类操作。
		开发商成员管理	机构管理员可对指定开发商进行开发商成员的管理维护，包括对开发商成员的查看、新增、编辑、删除。
		系统管理	为平台管理员（或机构管理员）提供政务系统的创建、编辑能力，以及政务系统管理能力的入口。
		角色管理	为平台管理员提供平台角色管理的能力。平台管理员可以为不同的用户指定不同的角色，通过基于角色的权限控制体系实现用户权限控制。包括平台管理员、机构管理员、机构成员、开发商负责人、开发商成员等。
		内容管理	为平台管理员提供【政务开放平台门户——资源中心】的业务新增、发布管理以及服务的增、删、改、查等能力。
		配置管理	为平台管理员提供可视化创建页面的管理

一级分类	二级分类	三级分类	功能特性
			工具，包括导航、功能菜单、页面元素等，通过简单的拖拽组件和定义组件之间的关联事件即可组装出系统页面。
	分项目控制台	分项目概况	对分项目概况内容进行开发任务发布，以及显示需要开发的应用情况、项目成员、开放能力、使用流程等信息。
		小程序应用管理	为机构管理员提供小程序应用的创建，支持小程序的版本管理、体验者管理、域名管理和基本信息管理。
		小程序开发管理	为机构管理员对已经创建好的小程序应用进行创建小程序主模块和子模块，创建时需要填写模块名称、仓库地址、负责供应商等信息，创建成功后能够生成独立的代码仓库地址，开发商可以在代码仓库进行小程序的应用模块开发，以及小程序的多模块在线合包和预览的功能，将不同的模块功能合并成一个独立的小程序并生成开发二维码，开发者可通过扫描二维码测试。
		申请审核管理	应用服务发布审核：开发商通过【政务开放平台门户——后台应用管理】提交应用服务发布申请后，由机构管理员进行审核，审核通过后开发商即可进行应用服务发布；
			第三方服务审核：开发商通过【政务开放平台门户——后台应用管理】提交第三方申请后，由机构管理员进行审核，审核通过后开发商即可使用该第三方服务；

一级分类	二级分类	三级分类	功能特性
			▲能力申请审核：开发商通过【政务开放平台门户——开放能力申请】提交能力申请后，由机构管理员进行审核，审核通过后开发商即可通过接入指南快速接入使用开放能力。
		IT 资源申请审核	开发商通过【政务开放平台门户——IT 资源申请】提交 IT 资源申请后，由机构管理员进行审核，审核通过后开发商即可使用响应 IT 资源申请。

2.3.3统一跨网数据交换平台

功能描述	模块	细分项
边界网关	工作模式配置	支持在不同安全密级的网络之间的服务注册发布及订阅。
		支持跨网闸、网络等安全边界设备的服务注册发布及订阅。
		支持基于文件双向交换模式实现跨安全边界访问；
		支持基于单向 TCP 协议模式实现跨安全边界访问；
		支持基于单向 HTTP 协议模式实现跨安全边界访问；
		支持基于数据库双向交换模式实现跨安全边界访问；
API 网关	创建服务	由服务提供方发起服务创建的过程，填写相关的

功能描述	模块	细分项
		服务配置信息，完成服务创建。
	服务发布审批	由系统负责人对服务创建的申请进行审批，只有审批通过之后的服务才能被允许订阅和调用。
	更新服务	如果某个服务的配置信息发生变化，可以对已经创建的服务信息进行编辑修改。
	删除服务	如果某个服务不再需要使用，可以对服务进行删除，删除后的服务不能继续被访问。
	发布服务草稿	如果某一服务不希望在编辑时立刻提交，可以将服务保存为草稿，处于草稿状态的服务不会产生审批单据，也可以随时编辑。
	服务禁用/启用	对已经创建的服务信息进行禁用操作，禁用之后该服务将临时停止对外服务。 如果需要重新对外提供被禁用的服务，则对该服务执行启用操作即可。
	服务冻结/解冻	对已经创建的服务信息进行冻结操作，冻结之后该服务可以对外服务。但是不能编辑。 如果需要编辑被冻结的服务，则对该服务执行解冻操作即可。
	服务标签	为服务打标签，可以做分组、编排等管理
	查看服务详情	查看已经创建的服务的详细信息
	搜索服务	在某一应用下搜索具体服务
	查看应用发布的服务列表	查看该应用下发布的所有服务及服务的状态

功能描述	模块	细分项
	创建服务	由服务提供方发起服务创建的过程，填写相关的服务配置信息，完成服务创建。
准入网关	创建站点	由站点提供方发起站点创建的过程，填写相关的站点配置信息，完成站点创建。
	站点发布审批	由系统负责人对站点创建的申请进行审批，只有审批通过之后的站点才能被访问。
	更新站点	如果某个站点的配置信息发生变化，可以对已经创建的站点信息进行编辑修改。
	删除站点	如果某个站点不再需要使用，可以对站点进行删除，删除后的站点不能继续通过里约代理被访问。
	发布站点草稿	如果某一站点不希望在编辑时立刻提交，可以将站点保存为草稿，处于草稿状态的站点不会产生审批单据，也可以随时编辑。
	站点禁用/启用	对已经创建的站点信息进行禁用操作，禁用之后该站点将临时停止对外服务。并展示对应的禁用页面。 如果需要重新对外提供被禁用的站点，则对该站点执行启用操作即可。
	发布路径转换配置	支持对原始站点地址和对外发布地址转换，对原始站点地址进行保护，不暴露给访问者。
	SSL 配置	支持 http 和 https 协议，同时可以对 https 证书进行检查
	流量控制配置	▲频次配额：支持站点分配调用频次上限，避免站点突然超量访问超出原始站点处理能力。 超时配置：支持配置最大响应时间，避免因某一

功能描述	模块	细分项
		服务无响应的原因一直占用服务带宽及等待时间；
	用户访问设置	支持某些特殊的场景，如小程序，支持用户直接访问 API，同时对来源身份进行校验
应用管理平台	创建应用	作为一个系统的内部应用模块存在，可根据业务系统的实际情况，在一个系统内部创建多个应用。
	根据分区设置 token	按照分区单独设置 token，不同分区的服务请求时需要使用对应的 token 进行签名
	更新应用	如果某个应用的信息发生变化，可对应用的相关信息进行编辑修改。
	查看应用列表	查看已经创建系统下的所有应用列表及应用使用服务的情况
	查看我的应用列表	查看某一应用负责人名下所有的应用
	查看应用详情	查看已经创建的应用详情
	查看	查看网络区域、分区和智能网关节点阵列信息
	查看	查看分区和智能网关节点阵列信息
	删除应用	如果某个应用不再需要使用，可对应用的相关信息进行删除操作，同时该应用下包含的服务也将同步被删除。当该系统下有未审批完的申请或者已经冻结、禁用的服务时，删除失败。
其他能力	多活部署	支持跨数据中心的多活部署模式，即便发生严重的数据中心故障，也可以通过同城或异地的容灾数据中心的备份服务持续提供对外的 API 服务能

功能描述	模块	细分项
		力。
	横向扩展能力	产品支持横向扩展集群化部署
	软件著作权	已申请成功 5 个软著证书。

2.3.4统一民生警务运营平台

一级分类	二级分类	三级分类	功能特性
运营数据中心	数据看板	全局看板	▲提供全省维度的全局数据看板总览，以数据统计、数据占比、趋势分析等运营统计手段，涵盖业务事项、访问量、用户等多维度的运营统计分析应用功能，从全局角度展现政务民生应用的整体运营情况。
		地市看板	提供以某个地市维度的地市数据看板总览，以数据统计、数据占比、趋势分析等运营统计手段，涵盖业务事项、访问量、用户等多维度的运营统计分析应用功能。
	概况分析	访问趋势	根据用户数据、访问数据两大维度按时间段进行趋势分析、区间比对分析，用户数据包括总用户数、实名用户数、新增用户数、新增实名用户数、公众号粉丝数，访问数据包括总访问量、访问人数。
		实时分析	根据某个页面的访问次数（PV）和访问人数（UV）进行页面实时访问趋势分析，以及某个页面的访问统计数及占比。
		活跃用户分	根据活跃用户人数（MAU），进行活跃用户人数

一级分类	二级分类	三级分类	功能特性
		析	趋势分析。
		用户画像	根据活跃用户、新增用户的用户分类方式，进行用户画像分析，支持自定义区间进行分析。包括用户属性分析、地区分布、终端和机型分布。
		用户参与留存	用户参与分析：根据分享次数、人均停留时间、次均停留时间作为用户参与的方式，进行用户参与趋势分析。 用户留存分析：根据活跃用户、新增用户的用户分类方式，进行用户留存百分比分析。
		访问来源分析	根据小程序的访问来源、访问时长、访问深度进行统计分析，支持自定义区间进行分析，有效调整系统运营模式。
	事项统计	事项普及度地市排行	根据服务事项的普及度进行地市明细查询，以及可以按照服务分类、业务范围、上线状态等进行查询统计，进一步了解服务事项的普及度能够加强服务事项的运营推广工作。
		事项查询/办理量统计	根据服务事项的查询/办理进行明细查询，以及可以按照服务分类、业务范围、主管单位、统计时间维度等进行查询统计，进一步了解服务事项的使用率、办结率，能够对服务事项的工作流程进一步调优。
		事项优化效果统计	根据服务事项的优化效果进行明细查询，以及可以按照服务分类、业务范围、上线时间等进行查询统计，进一步了解服务事项的优化效果能够对服务事项的工作流程进一步调优。

一级分类	二级分类	三级分类	功能特性
	指标达成	指标管理	对运营指标的目标里程碑进行管理及设置，指标设置项目包括日均访问量 PV（页面浏览量）、日均访问人数 UV（独立访问用户数）、累计用户数统计、服务事项总量、事项全省普及占比、累计业务查询办理统计分析等。
		指标查看	对已设置的运营指标按自定义时间维度进行查看。
运营管理中心	开发商管理		管理提供政务服务的开发商相关明细基本信息，支持新增、删除、修改、查询、导出表格数据功能。
	厅局委办管理		管理厅局委办等政务服务机构的明细基本信息，支持新增、删除、修改、查询、导出表格数据功能。
	业务系统管理		管理政务运营平台所需要运营的业务系统相关明细基本信息，支持新增、删除、修改、查询、导出表格数据功能。
	服务事项管理		管理服务事项的明细内容，支持新增、删除、修改、查询、导出表格数据功能。
	渠道分发管理		用于 URL、小程序码分发渠道管理，自动生成不同渠道的葵花码和 URL 链接，可统计不同渠道来源数量和评估渠道拉新效果。
	统计点管理		管理设置页面及自定义统计点，以及对统计点进行统计数据查询。
	用户积分管理		对接政务服务用户积分体系，提供积分数据支撑用户获取、消耗和留存积分分析。包括积分任务、积分商城、积分活动维护、积分管理以及积分数据报表功能。

一级分类	二级分类	三级分类	功能特性
用户管理	账号管理		对平台账号进行管理。
	权限管理		对账号权限进行管理。

2.3.5统一移动管理支撑平台

项目	招标要求
基本要求	平台支持多网络环境（如政务内/外网和互联网构成三网环境）的部署运行，支持与即时通讯平台通讯，支持应用（包括原生应用、H5 轻应用）发布上架，用户在应用市场客户端获取应用后，统一在即时通讯工作台打开应用。
功能性要求	提供统一用户中心对部门、用户、标签进行集中式统一管理
	支持部门、用户信息导入/导出、排序，支持对部门、用户的属性字段进行自定义扩展
	统一用户中心必须支持对接即时通讯工具的通讯录，实现在平台维护即时通讯通讯录的功能，同时支持复杂组织架构，包括多父节点、分管领导设置，支持设置不同管理员管理的组织架构范围（管理对象粒度可具体到某部门），
	实现统一用户认证管理体系，实现应用单点登录，认证因子包括支持普通帐密、即时通讯工具内置的扫码等鉴权方式、CA 认证、AD 域认证等。
	▲平台提供统一移动应用市场，支持对原生应用和 H5 轻应用进行统一的管理，包括支持应用创建、上下架、审核、发布及授权管理等。
	提供移动应用市场 App 客户端，提供应用分类浏览、应用排行、应用场景化专题、应用搜索、标签筛选、查看应用详情、应用反馈评论等功能。应用列表支持根据地域、警种、应用区域等类型分类展示。
	▲实现即时通讯工作台功能，用户在应用市场获取应用（原生应用、H5 轻应用）后，在工作台中显示我的应用列表，支持对应用自定义分组分类排序的个性化设置。
	提供应用市场后台管理，实现应用的上架、发布审批及授权操作，支持应用市

项目	招标要求
	场分级分权管理，为地市、警种创建子应用市场指定管理员独立管理。
	支持并实现 3 家运营商网络同时接入。
	支持通过公安部检测的多种安全监控组件同时接入并管理。
性能	支持多节点集群部署，提供稳定的运行保障，平台的可靠性可达 99.99%
	平台可支撑超过 3000 个应用的接入，接口日调用总量超过 1000 万次，并发调用峰值可达 700 次/秒，达到并发调用峰值时平均响应时间应小于 1 秒
	统一用户中心支持大型机构的深层级的组织关系，支持的组织架构人员数超过百万级，单次用户导入量可达 5 万，每次导入时间不超过 15 分钟
安全性	具备完善的安全设计，提供端到端安全解决方案方案，对传输链路加密、内容加密、数字签名，从而防止恶意监听、重放和暴力破解。
	对服务端数据加密，敏感数据加密落地存储，账号密码采用不可逆的 hash 算法加密，实现数据被泄露后依旧不能查看
	通过接入网关和准入网关保障请求合法性，所有的访问调用过程记录调用日志，可对请求进行追溯

2.3.6统一公安可信认证平台

序号	指标项	技术参数要求
1.	算法资质	-提供 20 项以上 OCR、人脸识别相关的专利证明。 -OCR、人脸识别相关领域国际权威竞赛排名第一证明。
2.	数据源资质	-支持对接公安部身份证号码查询服务中心和公安部第一研究所人脸库权威数据源，并提供比对服务接口。
3.	活体检测能力	-支持活体检测能力，可抵御照片攻击、视频（翻拍或合成）攻击、3D 纸片面具攻击等多种攻击手段。 -真人活体检测通过率大于 95%。 -支持配合式的活体检测（动作、数字）及非配合式的活体检测（反光、静默） -支持不同活体检测模式一键切换。 -支持微信端活体检测的摄像头浮层能力。

序号	指标项	技术参数要求
4.	人脸识别能力	-支持在误报率千分之一的情况下，人脸比对通过率大于 97%。
5.	平台支持	-支持移动端 iOS、Android、微信小程序、公众号 H5 等多平台。
6.	平台运营	-支持微信端的帐号体系风控能力。 -支持微信支付实名再校验。 -支持黑名单限制能力。 -支持数据统计及运营管理。
7.	部署形式	-支持活体检测、封装公安部一所签名服务器接口，实现与权威资源的人像比对。
8.	并发能力	-支持 300QPS 以上并发数。
9.	案例要求	-需提供相似案例的合同三份以上。 -需提供公安行业相似案例上线服务号十个以上。
10.	资质要求	-须提供产品的软件著作权证书复印件，并加盖原厂商公章。 -须提供产品功能、准确率的第三方测试报告，并加盖原厂商公章。

2.3.7统一智能客服平台

功能描述	模块	细分项
智能客服平台	智能客服系统	机器人构建与管理，查询机器人状态
		权限管理，操作人员权限管理
		数据统计，基于日常智能客服运行状态，进行机器人接入数量、反馈时间、准确率等进行统计展示
	知识库机器人	构建多机器人实例，可根据相同或不同 FAQ 知识库进行构建
		单机器人可支持 100qps 咨询业务并发，反馈时长 300ms 内
	知识图谱机器人	基于知识库构建业务知识图谱，实现业务关联推荐和多轮问答回复
	多层级语料库管理	支持二级分类知识库构建与管理，支持同义词导入扩展
		支持行业通用知识库管理与导入添加

	警务知识库整理	结合警务行业通用知识和业务知识进行整理，实现指定区域警务知识的快速模板导入即可使用
	知识库智能学习	支持相似问学习，自动发掘相似问，一键加入知识库
		支持未知问题学习，自动聚类挖掘未知相似问题，一次编辑即可批量导入知识库
		不满意问题学习，对不满意问题进行人工学习优化后加入知识库
	多渠道接入	支持微信公众号、微信小程序、APP、PC 网页和 H5 等渠道接入

2.3.8互联网中间件服务能力集成

本期项目建设业务能力支撑层主要提供以下相关的服务能力。

2.3.8.1 集成申办受理平台

依据规划建设，各警种申办受理平台，需要在工作流引擎平台上建立外网的预约、申办、受理，内网的申办受理服务，省公安厅主要以集成平台相关接口，并为海南公安省市单位提供申办受理接口对接支持。

2.3.8.2 统一支付业务能力

统一支付是海南便民惠企警务提升服务质量，增加用户舒适度的重要举措之一，旨在针对民生服务里涉及收费流程业务事项，提供网上缴费，为社会公众办理缴纳公安非税收入等公共收入提供支撑平台。

海南公安统一支付以互联网支付为主要支付工具，通过打通互联网支付、非税系统的相关接口实现统一支付功能。

2.3.8.3 物流平台

物流平台集成智能快递查询、快递状态智能推送、快递网点查询、快递时效查询等多项创新性服务为一体的快递物流服务平台，物流平台集成多家快递物流公司的快递查询能力，提供统一、稳定的快递查询能力，开发商可快速接入。

2.3.8.4 集成互联网地图服务

提供地图、定位、地点搜索和路线规划能力，并可基于海量位置数据和人群动态数据。

2.3.8.5 集成政府授权的第三方服务

对于各警种普遍都需要用到第三方服务，政府授权后，以集成的方式统一对外提供服务。

2.3.8.6 服务集成电子证照

配合省工信牵头的电子证照系统，调用省厅电子证照身份信息，并以省厅为单位集成电子证照服务能力，并为各警种提供服务支持。

2.3.8.7 集成政府业务系统开放能力

政务业务系统的公共服务能务，省厅集成后，统一对外开放提供服务

2.3.8.8 电子印章应用能力

根据海南便民惠企业务规划，需提供无犯罪记录证明等便民业务，这些业务需要通过电子签章等安全技术手段保证真实性,避免了纸质证照伪造的可能。

基于此业务需求，要求对电子印章系统进行集成，能够很便捷地或自动为

便民惠企平台提供数据的支撑。

2.3.9私有化中间件服务建设

2.3.9.1 OCR 服务

提供 OCR 图像识别软件，支持客户端识别和服务器端识别服务，包括证件识别（身份证、护照、驾驶证、行驶证等）、车牌识别等。

身份证识别接口支持二代身份证正反面所有字段的识别，包括姓名、性别、民族、出生日期、住址、公民身份证号、签发机关、有效期限；具备身份证照片、人像照片的裁剪功能和翻拍件、复印件的识别告警功能。应用场景包括：银行开户、用户注册、人脸核身等各种身份证信息有效性核验场景。

2.3.9.2 位置服务

整合定位、地图、地点搜索、路线导航、热力图等多种基础能力。

提供热力图直观页面展示、定位 SDK、地图 Web 组件、API 等灵活接入方式。

热力图功能可快速展示实时分析结论，交互界面生动直观。

2.3.9.3 短信服务平台

满足交警、治安、出入境等警种的短信服务平台。

2.3.9.4 通用 mPaaS

移动端原生应用开发框架、移动端 H5 应用开发框架、移动端原生应用插件框架、后台微服务框架

2.3.9.5 通用应用开发框架

Web 开发框架旨在提供一套较为完整的视觉设计、UI 交互、数据邦定等开

发组件，提升业务应用的开发效率，使每个业务 Web 应用有统一的使用体验和开发模式。

2.3.9.6 微服务

序号	指标项	技术参数要求
1	支持 Spring Cloud、Dubbo 应用	支持使用 Spring Cloud 的框架开发的应用，兼容 Dubbo 框架开发的应用。
2	支持 Service Mesh 应用	支持多种语言开发的 Service Mesh 框架。
3	容器、虚拟机集群管理	用户可以选择使用容器或者虚拟机部署应用。
4	镜像仓库、软件仓库管理	-
5	服务注册发现	提供基于服务自动注册发现，满足 spring cloud 与 service mesh 基于注册发现的互访。
6	负载均衡	-
7	权限控制	通过权限控制模版灵活控制敏感操作权限，保证数据、应用安全。
8	租户隔离	不同租户间信息隔离，互不影响。
9	配置推送	应用配置、全局配置、日志配置等相关配置的下发、版本管理，支持文件上传、数组、yaml 等格式配置。
10	系统、服务级别监控与告警	服务数据、日志级别监控，Dashboard 配置。
11	生命周期管理	支持应用的部署、起停、回滚、升级、扩缩容等能力。
12	打通腾讯云中间件消息队列、API 网关服务	-
13	日志查询与监控	结构化监控业务日志，灵活配置告警通知到手机、邮箱。支持基于自定义标签查询
14	服务依赖拓扑	支持服务依赖拓扑图展示，调用链分析，方法追踪，调用链标签。

2.3.9.7 工作流引擎服务

工作流引擎包括对工作流的定义、工作流的权限分配、工作流的使用、工作流的运行状态管理等进行支撑。

2.3.10 统一运维管理平台

序号	模块	功能	说明

序号	模块	功能	说明
1	总体设计	技术架构	1、基于主流开源平台 Zabbix 最新稳定版本深度开发实现 2、系统前端采用 bootstrap v3+vue2.x，后端采用开发的 PHP5.6 架构 3、采用分布式部署，支持二级代理横向扩展 4、支持二次开发(代码可开源) 5、支持用户自定义指标扩展 6、支持数据库双重高可用设计
2	全局视图	监控总览	1、提供全局视图功能，对监控对象、告警状态进行分类管理 2、展示监控对象的关键数据，总览监控设备状态
		指标排行	1、提供重点指标排行功能，对于重要监控指标，可将数据进行 Top5 排行 2、提供即时查看排行中单个数据曲线图 3、提供跳转对象详情界面，以便运维工程师掌握监控对象的整体性能 4、提供图形化展示重点指标 Top5 排行
		严重告警	1、提供最新严重告警首页展示功能，新告警自动刷新，可以及时发现对象的异常状态并处理 2、提供近 30 天严重告警统计的同比和环比功能（统计近一个月严重告警的数量，并且与之前一个月进行告警环比），展现形式曲线图
		快速创建	1、提供创建监控对象的快捷方式，支持 WEB、主机、网络设备、数据库、中间件、应用、硬件、虚拟化、链路等
		今日概况	1、提供概况信息统计功能，包括今日新增、关闭的告警数量及不同方式发出通知数量 2、支持按照通知方式分类统计通知条数，用户可根据每个渠道发送条数初步判断通知渠道是否异常
		运行状态	1、 提供监控运行状态实时展示，方便查看当前服务器的采集状态、用户数、总监控项及总触发器
		维护清单	1、 提供设备快速加入维护清单功能（加入维护清单可选不采集数据，那么在维护期间内维护设备异常则不发送告警通知） 2、 展示已在维护期内的设备信息

序号	模块	功能	说明
3	实时告警	告警展示	1、告警列表支持当前告警、历史告警、三方告警三种分类展现方式（三方告警集成了市面上大部分监控软件的标准接口，可以快速和其他监控平台进行对接，方便用户集中管理所有告警） 2、提供告警信息统一功能、集中展示，支持告警信息按照严重级别、开始及结束时间、设备类型、确认情况、维修情况等筛选功能，支持告警关键字搜索功能 3、提供告警历史分析功能，包括告警产生时间、恢复时间排行、告警确认信息，将处理过的历史告警收集成列表供分析使用 4、提供告警的确认历史功能，包括确认时间、确认人、确认信息、确认操作等信息。 5、提供告警发送通知的查看功能，包括告警类型、发送时间、发送方式、接收人及发送结果等信息 6、告警信息包括：名称、设备、IP 地址、产生和恢复时间、故障原因和解决方案、监控点、状态值等信息 7、告警状态可针对级别、标题、对象名、IP 地址、时间、时长、确认信息进行排行 8、提供告警的确认和通知的次数查看 9、提供预警告警的设置，即根据一定时间内的规律预测未来多久达到峰值的指标 10、提供告警声音配置面板，支持利用电视机声源进行声音告警，支持按照告警级别不同发出不同的声音
		告警管理	1、提供告警管理功能，可配置告警触发阀值设置功能 2、提供告警触发原因和解决方案配置收集功能 3、提供告警信息确认和提交关闭等维护功能，支持批量维护功能 4、提供告警导出功能（导出支持当前页、选中的、全部三种模式） 5、支持批量确认告警
		专家智库	1、提供告警关联专家智库功能，运维人员将故障处理方式记录到专家智库，这些信息将通过算法自动匹配到告警列表，为运维人员下次处理类似告警提供参考依据

序号	模块	功能	说明
			2、支持对专家智库信息进行点赞和点踩，专家智库的匹配算法会根据用户点赞和点踩的行为进行智能匹配告警 3、支持查看最高赞和最新回答的专家智库信息
		告警推送	1、提供告警提醒推送功能，将告警信息及时下发给运维人员 2、支持短信、邮箱、微信、钉钉等告警推送方式，支持对接 ITSM 或其他 IM 渠道 3、可以设置不同角色、不同告警对象、不同告警级别以不同的告警方式发送告警信息，并且用户可以在系统中配置告警内容模版 4、所发送的告警通知提供收集管理功能，能够针对推送出去的告警跟踪管理 5、通知方式支持告警产生的时候发送通知和告警恢复的时候再次通知，让 IT 经理做到心中有数
4	监控功能	监控列表	1、提供对象列表管理功能，支持对象名称、业务别名、IP 地址、启动监控、状态、类型、备注和标签等信息设置、操作和排序功能 2、支持对象信息检索，支持类型、是否监控、对象分组及对象类型的分类检索 3、支持新增对象，删除对象、修改、删除、批量删除等操作 4、支持对监控对象进行快速维护的操作及资产信息的配置等操作 5、提供批量导入功能，可以对所有对象的对象模板先下载并修改后进行批量更新操作，针对主机、网络设备、中间件、数据库和应用等对象模版导出，对象模板批量导入等批量更新管理功能 6、支持批量修改功能，支持模板类型选择功能，若是 web 类型的对象可以批量修改设备类型 7、支持监控对象的导出功能，支持导出当前页、选中项、全部数据三种方式 8、支持对监控对象打上一个或多个标签，支持“且”和“或”的逻辑关系进行标签搜索 9、支持批量对象归属，划分对象归属后，普通用户只能看到自己名下的监控对象，方便进行管理，超管用户还是可以看到所有监控对象 10、支持批量修改对象的分组信息（替换分组、追加分组）

序号	模块	功能	说明
		WEB 监控	1、提供 WEB 监控功能，针对响应时间、响应代码、状态码、速率、错误信息监控 2、提供历史监控信息曲线图分析功能，曲线图时间点可自行设置 3、支持监控 http、https、接口等模拟登录操作 4、支持模拟一系列基于 BS 架构的用户登录，用户操作和查询等业务操作流程仿真 5、支持批量删除监控对象 6、支持 WEB 对象连续添加（一个对象添加完成后不关闭弹窗，方便用户连续添加多个对象）
		主机监控	1、提供主机监控功能，针对运行状态、运行时间、CPU 使用率、内存使用率、磁盘使用率、磁盘总量和使用量、网卡发送和接收速率等进行监控 2、提供主机所运行的服务自动发现和状态监控的功能 3、支持 windows、IBM Aix、Red-hat Linux、HP Unix、Sun Solaris、Novell SUSE、CentOS、FreeBSD、Redflag Linux 等主机操作系统 4、支持自动获取主机的配置信息，精准、有效、及时地录入 IT 系统，详情直接展示资产配置信息，无需弹框，界面更直观，且在详情界面可直接修改配置信息，对象列表同步更新内容 5、支持主机自定义监控指标的添加、删除等操作 6、提供服务器的进程信息，包括进程的线程 ID、CPU 和内存的使用率等信息 7、提供当前服务器的所有指标的详情信息，包括文本历史、图表的展示 8、支持监控概要面板小部件化自定义，可拖拽
		网络设备监控	1、提供网络设备监控功能，针对运行状态、CPU 使用率、内存使用率、端口发送和接收总流量、端口发送和接收速率、端口发送和接收丢包率等指标进行监控 2、提供端口发送和接收速率、端口发送和接收丢包率、对比图标显示 3、支持网络设备包括交换机、防火墙、负载均衡等，支持思科、华为等品牌，以及设备上的所有网络端口，用户可以对网络资源进行管理上的分组 4、支持手动单个和批量关闭、启用端口监控，查看端口管理界面支持一目了然看到所有已监控和未监控的端口号

序号	模块	功能	说明
			5、支持自动获取网络设备的配置信息，精准、有效、及时地录入 IT 系统，详情直接展示资产配置信息，无需弹框，界面更直观，且在详情界面可直接修改配置信息，对象列表同步更新内容 6、支持自定义网络通讯设备监控指标的添加、删除功能，用户可以自行设置在详情界面展示的指标趋势图 7、支持监控概况面板小部件化自定义，可拖拽 8、支持关联资产信息，监控能读取到的信息会自动填写
		存储监控	1、提供存储监控功能，针对运行状态、CPU 使用率、内存使用率、IO 速率、RAID 状态、温度、电源、风扇等 2、支持监控 IBM、华为、惠普、戴尔、联想等主流品牌 3、监控指标支持自定义设置
		数据库监控	1、提供数据库监控功能，针对数据库服务状态、进程数、连接用户数、活动状态、活动会话数、数据库死锁数、数据库 BUFFER 命中率、数据库作业数、数据库用户连接数、数据库文件大小、数据库文件启动事务数、查询状态和发送状态等信息监控。 2、支持监控 MySQL、Oracle、MongoDB、PostgreSQL、SQL Server、Oracle RAC、Sybase、DB2 等数据库 3、自动获取数据库的配置信息，精准、有效、及时地录入 IT 系统，详情直接展示资产配置信息，无需弹框，界面更直观，且在详情界面可直接修改配置信息，对象列表同步更新内容 4、针对于 Oracle 类型数据库，支持 Oracle 数据库的慢 SQL TOP10、数据库死锁、会话 TOP10、表空间等信息的展示 5、支持数据库自定义监控指标的添加、删除功能，用户可以自行设置在详情界面展示的指标趋势图 6、支持监控概要面板小部件化自定义，可拖拽

序号	模块	功能	说明
		中间件监控	1、提供中间件监控功能，针对 Tomcat 指标有 Tomcat 版本、当前活动会话数、被拒绝的活动数、活动会话最大数、程序请求数、每秒收到和发送的字节数；IIS 指标有 IIS 版本、IIS 当前连接数、每秒 GET 请求数、每秒 POST 请求数、每秒 HEAD 请求数、ASP.NET 请求数等, 针对 Kafka 指标有消息消费以及同步，生产的延时、耗时， 当前线程数、线程数峰值、总消息进出速率、Partition 的 IO 速率以及拥有的 Topic、GC 计数器 等，针对 Flume 的指标有 Channel 名称以及 Channel 使用百分、消息总推送数量，成功推送以及失败数量、消息总接收数量，成功接收以及失败数量 Skins 名称以及写入数量跟连接失败计数，Sources 名称以及消息传输量等 2、支持 IIS、Tomcat、Apache、WebSphere、EAServer、JBoss、WebLogic、Nginx 等中间件 3、支持自动获取中间件的配置信息，精准、有效、及时地录入 IT 系统，详情直接展示资产配置信息，无需弹框，界面更直观，且在详情界面可直接修改配置信息，对象列表同步更新内容 4、支持中间件自定义监控指标添加、删除功能，用户可以自行设置在详情界面展示的指标趋势图 5、支持监控概要面板小部件化自定义，可拖拽
		应用监控	1、提供应用监控功能，针对应用响应时间、应用加载速度、应用日志错误监控 2、支持监控 LDAP、Exchange、FTP、SMTP、POP3、DNS、DHCP、Asp.Net、JVM 等标准应用 3、支持自动获取应用的配置信息，精准、有效、及时地录入 IT 系统，详情直接展示资产配置信息，无需弹框，界面更直观，且在详情界面可直接修改配置信息，对象列表同步更新内容 4、支持应用自定义监控指标添加、删除功能，用户可以自行设置在详情界面展示的指标趋势图 5、支持监控概要面板小部件化自定义，可拖拽

序号	模块	功能	说明
		硬件监控	1、提供硬件监控功能，针对运行状态、指示灯、IO 速率、raid 状态、温度、电源、风扇等 2、支持监控 IBM、惠普、戴尔、华为、联想、浪潮和曙光等品牌 3、支持自动获取硬件的配置信息，精准、有效、及时地录入 IT 系统，详情直接展示资产配置信息，无需弹框，界面更直观，且在详情界面可直接修改配置信息，对象列表同步更新内容 4、支持硬件自定义监控指标添加、删除功能，用户可以自行设置在详情界面展示的指标趋势图 5、支持监控概要面板小部件化自定义，可拖拽
		虚拟化监控	1、提供虚拟机监控功能，支持运行状态、CPU 使用率、内存使用率、磁盘使用率、磁盘总量和使用量、IO 速率等 2、支持监控所有主流虚拟化平台 3、支持监控所关联的所有虚拟机的信息，包括 CPU、内存、硬盘的使用率、状态等，支持看看各个虚拟机的指标信息 4、支持虚拟化自定义监控指标添加、删除功能，用户可以自行设置在详情界面展示的指标趋势图 5、支持监控概要面板小部件化自定义，可拖拽
		云平台监控	1、 支持监控所有主流云平台 2、 提供如云服务器的运行状态、CPU 使用率、内存使用率、磁盘使用率、磁盘总量和使用量、IO 速率等监控指标 3、 全方位覆盖计算、存储、网络、数据库等云平台产品的负载和性能监控指标 4、 支持混合云监控，多云、云上、云下多重环境基础监控 5、 支持自定义监控指标添加、删除功能，用户可以自行设置在详情界面展示的指标趋势图
		链路	6、 支持链路监控功能，针对链路的带宽及其使用率进行监控 7、 监控信息包含：名称、端口、上行带宽、下行带宽、带宽利用率等 8、 支持 B 端的自定义填写运营商名称 9、 支持新增、删除、修改、批量删除链路等操作 10、 支持端口不存在监控列表中界面给出相应展示信息 11、 支持自定义链路分组功能
		其他监控	1、Docker、微服务等监控

序号	模块	功能	说明
		监控管理	1、提供监控对象分类管理功能，提供标签设置功能，提供监控对象核心指标排行功能，其中包含主机的严重告警、CPU、内存、磁盘；网络的严重告警、接收速率、发送速率、接受丢包率、发送丢包率等；数据库的严重告警、表空间、用户连接数、每秒查询数等；中间件的严重告警、连接数、会话数和总访问量等，并且可即时查看排行中每个对象的状态曲线图 2、提供监控对象最新严重告警首页展示功能，新告警自动刷新，可以及时发现对象的异常状态并处理；提供严重告警统计和同比功能，统计近一个月严重告警的数量，并且与之前一个月进行告警同比 3、可根据小部件自定义主机监控的概况面板，提供单台监控对象监控概况全局显示，提供核心信息自定义显示，包含主机最新告警、运行服务、CPU、内存、硬盘和网卡等，网络设备端口、读写速率等，支持列表、曲线图、饼状图、柱状图等多种显示方式，相关指标的时间区域可通过滑块灵活调整 4、提供监控对象资产信息管理功能，资产信息可录入、修改、导出等功能 5、支持监控对象检索功能，支持部分核心数据导出功能 6、管理面板支持在迁移模板的时候选择默认面板和不使用面板（支持根据客户需求定制面板）
5	视图功能	最新数据	1、 支持根据主机群租、主机、应用集、名称等信息对最新数据进行筛选 2、 最新数据支持列表展示和图形展示 3、 支持显示堆叠数据图和折线数据图
		一览视图	1、提供一览视图功能，针对所选对象指标列表一览 2、可按照监控对象、分组、标签方式选择显示，支持多选功能 3、支持导出一览视图列表中的数据 4、支持全屏查看一览视图的数据信息 5、支持保存历史查询记录，方便用户下次快速查询
		网络拓扑	1、提供网络拓扑图功能，提供基于 Zabbix 的拓扑自动发现功能 2、支持多个拓扑图分类新建，支持拓扑图自定义配置以及按照业务细分 3、支持手动添加对象及自动发现拓扑图，自动发现功能又包含静态发现和动态发现，动态发现的过程中可以实施停止发现操作

序号	模块	功能	说明
			4、开启告警： 1）当前拓扑会对拓扑对的所有对象进行周期性的告警获取，如果存在告警，拓扑的对象会按照告警的级别进行特定颜色闪烁 2）拓扑的所有对象可以进行鼠标双击查看告警列表 3）拓扑链路可以进行鼠标双击查看链路信息，包括端口、端口状态、上下行端口宽带利用率等信息 4）支持绑定链路监控，当链路达到告警阈值时，链路会按照告警的级别进行特定颜色的闪烁 5、拓扑图支持主机、网络、虚拟化和链路 6、提供拓扑图能够动态实时反映拓扑图中设备和链路运行状态情况 7、提供拓扑图中设备和链路核心信息快速访问显示功能，包含名称、IP、状态、告警、速率等信息 8、实现当某个监控对象有故障时，可以实现双击对象图标弹出告警信息列表框，便于迅速检查性能及告警数据 9、支持拷贝拓扑图的功能，便于区别不同的用户之间的不同的展示方式 10、支持右键方式对监控对象进行排列格式化，能达到局部区域显示的规格化布局，实现美化排版的目的 11、支持右键方式对监控对象进行更新对象、端口信息、执行脚本的操作和查看功能。 12、支持右键方式调整到监控对象的详情界面 13、支持画布右键添加子网、设置背景、移除背景、添加图例和清空画布的操作 14、支持自动排查当前自动生成的拓扑图功能，哪些设备已经加入监控，哪些设备未加入监控，如果未加入监控的对象允许用户实现一键纳入监控 15、支持拷贝网络拓扑图功能，便于区别不同的用户之间的不同的展示方式
		业务地图	1、提供业务地图功能，展现业务系统与网络设备、数据库、服务器等的树状关系图，实现业务故障的快速定位 2、提供单个业务负载情况、健康度、可用性监控功能

序号	模块	功能	说明
			3、提供业务地图中设备和链路核心信息快速访问显示功能，包含名称、IP、状态、告警、速率、端口、端口状态、接收和发送丢包率等信息 4、支持拷贝业务地图并调整展示方式，可自行命名拷贝的业务地图，方便查看 5、对象存在告警时，优化了监控对象闪烁功能，对象会按照告警的级别进行特定颜色闪烁 6、 支持鼠标双击对象可以查看告警列表 7、 支持各个业务地图直接的引用功能 8、持右键方式对监控对象进行星状格式化、单独调整字体大小、更新、删除及进入到监控对象的详情界面等操作 9、查看故障快照的功能，可直观对比分析异常指标的性能趋势，故障快照支持查看故障发生时的多项指标状态，方便运维人员进一步定位故障根源 10、业务地图可根据业务的重要性按照 A+级、A 级、B 级进行分类
		投屏视图	1、提供大屏背投视图功能，实时掌控监控状态，对不同的监控资源进行体现，将监控系统一键投到电视屏幕 2、提供投屏的自定义功能，按照需求自定义显示相关内容 3、支持定义一个投屏多个页面的自动切换，支持自定义多个页面切换时间 4、支持主题化、个性化设置 5、支持自定义背景 6、支持全屏效果展示 7、支持图表展示的默认样式应用功能 8、支持自定义设置投屏背景透明度 9、支持自定义图表展示数据的样式显示
		图形视图	1、支持图形视图功能，支持添加对象数据。 2、支持数据按照不同时间段进行缩放查看，支持多数据查看。 3、提供图形视图功能，用户可自行设置需要展示的指标的图形视图 4、支持不同对象的不同指标的图形视图的展示 5、支持根据图形名称搜索图表

序号	模块	功能	说明
			6、支持自定义图形名称
6	专家智库	智库管理	1. 提供专家智库管理功能，支持对专家智库知识标题、发布时间、发布人、点赞数、被踩数、评论数的管理 2. 专家智库信息来源包含：原始的主流处理方案建议和使用过程中记录的故障处理的触发原因和解决方案 3. 支持对专家智库信息进行点赞和踩功能 4. 支持对专家智库信息进行评论的功能 5. 支持新增、修改、删除、批量删除功能
		用户排名	1、 支持对所有用户的智库信息的统计功能 2、 支持查看各个用户的知识数量、点赞知识数、被踩知识数、知识点赞率、累积点赞数、累积被踩数、累积评论数等信息 3、 支持查看单独某个用户的所有知识信息
		专家主页	1、 支持查看当前登录用户的智库信息，包括知识数量、被赞知识数、被踩知识数、点赞比率、累积被赞数、累积被踩数 2、 支持查看所有用户发布的知识的排行榜信息，包括用户发布数 Top5、知识点赞率 Top5、知识评论数 Top5、点赞知识数 Top5、最多评论数 Top5 的排行榜信息 3、 提供新增知识的统计和同比功能，统计近一个月新增知识的数量，并且与之前一个月进行知识的同比
7	统计报表	告警统计	1、提供告警统计报表功能，统计一段时间内不同类型资源的不同级别的告警数，按照日、月、年和时间自定义设置方式统计 2、提供告警分类统计，按照 web、主机、网络、存储、数据库、中间件、应用、硬件和虚拟化分类统计功能 3、提供告警标题统计，针对 web、主机、网络、存储、数据库、中间件、应用、硬件和虚拟化进行统计，形成图标显示，支持图表单独显示和导出保存功能 4、提供监控项目告警统计，按照名称、IP 地址、告警标题、严重性和次数进行统计，支持按照以上指标排序功能

序号	模块	功能	说明
		日报周报月报	1、提供日报、周报、月报统计报表功能，支持对过去 24 小时、自定义日报、过去 14 天、自定义周报的运维状态统计形成报表 2、报表支持监控资源概况、告警统计（图形展示）、严重告警详情等内容的展示 3、支持报表自定义时间节点自动生成 4、支持日报周报月报按照时间筛选，支持告警记录检索功能，可重复查看和下载 5、报表支持导出 HTML 格式 6、自定义日报和自定义周报支持对报表进行自定义命名 7、自定义日报和自定义周报支持自定义时间周期 8、报表发送设置支持分别设置日报、周报、月报的接收人
		综合对比	1、提供指标的综合对比功能，支持相同类型的对象的指标的综合对比功能，可以是多个对象也可以是多个指标的对比，以列表的形式展示出指标的最小值、平均值、最大值用户可自行设置 2、支持综合对比指标的订阅情况，可根据实际情况自行设置订阅的具体情况，包括订阅模式及订阅时间等信息 3、支持 HTML、CSV、文本、Excel、PDF、JSON 等格式导出
8	系统管理	常规设置	1、支持界面设置、管家、图片、图标映射、正则表达式、宏、映射值、工作时间、触发器设置、触发器显示选项、其他设置
		宏值对照	1. 提供本地宏翻译的功能 2. 翻译过后的宏在用到宏时候显示的是中文（提高产品的易用性） 3. 宏翻译支持三种值类型（文本、数字、密码）
		自动发现规则	1、提供自动发现管理功能，针对自动发现规则进行管理 2、支持自动发现信息检索，支持类型分类检索 3、支持已发现设备、已检测的主机，在线和短线时间管理功能
		模板迁移管理	1、提供模板迁移管理面板 2、支持查看模板 ID 和模板名称 3、迁移模板支持选择模板的插件类型（是作为主模板还是附加模板） 4、迁移模板支持在面板显示和不显示两种模式 5、迁移模板支持选择默认面板和不使用面板两种模式

序号	模块	功能	说明
			6、支持根据类型、子类型、面板类型、模板类型等条件对模板进行搜索 7、支持对模板进行还原迁移和批量还原迁移 8、支持对当前系统中所有的模板状态进行筛选（例如全部未迁移的模板、主机在使用的模板、未被链接的模板等）
		ZBX 模版管理	1、提供模版管理功能，针对名称、应用集、监控项、触发器、自动发现、连接的模版等信息进行操作 2、支持模版信息检索，支持类型分类检索 3、支持应用集、监控项、触发器、自动发现等一系列的新增、修改、设置等功能
		通知配置	1、提供告警通知配置管理功能，支持针对名称、条件、操作和状态进行设置和删减 2、支持配置信息检索，支持类型分类检索 3、可以设置不同的类型资源在不同级别的告警产生及告警恢复下以多种方式（包括短信、邮件、微信）下发提醒消息给指定的多个用户，客户对配置进行禁用和启用 4、支持企业微信部门告警方式管理（配置微信群发）
		维护模式	1、 提供维护管理功能，针对名称、数据收集、描述、启用和状态进行设置 2、 支持新增和批量删除功能，加入维护模式的监控对象，不发送告警，并可自由设置是否收集监控信息，当设置有数据采集的情况下，设置维护期间如果产生告警则会等到维护期间结束后统一发送给下线客户 3、 支持针对名称、数据收集、描述、启用和状态排序功能 4、 支持同志配置信息检索 5、 支持类型分类检索
		用户管理	1、提供用户管理功能，支持登录名、手机、微信、密码、角色、有效期及是否能登录 Zabbix 等管理功能 2、支持用户新增、删除和批量删除功能 3、支持根据登录名或名称检索功能 4、支持角色的授权功能 5、支持批量删除功能
		权限配置	1、提供权限配置功能，统计报表、首页、告警、监控对象等各个功能权限设置

序号	模块	功能	说明
			2、提供角色的新增、删除及角色设置权限的功能 3、支持角色的检索功能
		对象分组	1、提供对象分组管理功能，支持对象分组名称、对象和删除管理 2、支持分类选择，支持信息检索操作 3、支持批量删除对象等的操作 4、支持剪切和插入功能（对分组进行快速排序）
		标签管理	1、 提供标签的管理功能，支持新增、编辑、删除、批量删除等操作 2、 支持剪切和插入功能（对标签进行快速排序） 3、 支持批量打标签功能（针对某一个标签批量分配给多个监控对象的功能）
9	系统配置	操作审计	1、提供操作日志记录功能，针对用户、请求途径、IP 地址、操作和时间进行记录 2、支持用户、IP 地址或反馈信息、创建时间的信息检索操作 3、支持选择审计来源进行查询（默认来源和 zabbix 审计来源）
		通知记录	1、提供告警通知记录功能，针对告警标题、接收方式、接收人、消息内容、发送时间、发送结果和失败原因进行记录和统计 2、支持告警记录按照时间筛选 3、支持告警记录按照标题、接收人、发送时间、发送结果的检索功能 4、默认查询当天的通知记录
		发信配置	1、 提供全局发信配置功能，针对邮件、企业微信、短信的发信通道参数进行配置 2、 支持测试邮件发送、测试企业微信发送、测试短信发送
		菜单配置	1、 支持用户新增自定义菜单（菜单名称、路由、图标、排序等信息都可以自定义） 2、 支持批量删除菜单
		全局配置	1. 支持配置系统名称、备案号、系统 logo、系统 icon 等信息 2. 问题反馈，支持一键跳转至官方论坛进行问题反馈（方便用户学习了解整套系统） 3. 版本信息，支持查看授权信息（授权对象、授权监控数量、授权使用天数等） 4. 支持更新、备份授权码信息 5. 支持修改用户密码 6. 支持清除缓存 7. 支持全局搜索监控对象（支持对 IP 和对象名称进行搜索） 8. 支持换肤（标准版和暗黑版）

序号	模块	功能	说明
10	微信客户端	微信推送	1、提供微信告警推送功能 2、用户配置告警提醒信息通过微信方式，系统产生对应的告警将会推送到用户的微信账号 3、用户可以查看告警详情，及时处理故障 4、获取监控平台未处理的告警信息，实时关注告警状态。 5、用户通过微信企业号进入主机监控、网络监控、应用监控，可以查看所有主机资源、网络资源、应用资源的当前状态，以及对应的详细性能信息。

2.3.11 系统软件及其他工具软件

投标人根据自己技术方案编制情况，列明需要的操作系统、数据库、中间件。

规格配置	单位	数量
Windows 2012 Server 标准版	套	4
CentOS 7.0 64 位或以上版本	套	171
Mongo 数据库 4	套	8
MySql 数据库 5.7	套	12
Redis 数据库 3.2+	套	8

2.3.12 关于业务逻辑与数据流定义的说明

- 移动互联网服务子平台（Ⅰ类区）网络

Ⅰ类网主要存放用户的注册信息；临时存放业务数据，包括群众在访问微信端时提交的数据。Ⅰ类网数据绝大部分是需要进入后台审批的，在这里为了做一个数据保护,所以Ⅰ类网中的数据会被备份一份在Ⅰ类网部署的服务器中，

防止出现数据错误、数据冗余、数据不同步。

- 联网服务子平台（Ⅱ类区）网络

Ⅱ类网中的数据主要是进行数据流转的，为了安全考虑，公安的网络是做了严格的限制与区分的，该网络段中的数据进行加密与解密处理后将流转至公安内网。

- 公安信息网服务子平台（Ⅲ类区）网络

Ⅲ类网中的数据从业务上区分为两类，一类是微信端传递过来的数据，这类数据是需要进行处理与审批;一类数据是审批后台与内网需要进行审批处理、统计查询、操作管理所需要的数据，这些数据在内网交互时采取文件的格式，以保证数据的安全性与可靠性，降低系统性风险。

2.4 应用系统对接

2.4.1便民惠企应用方面

2.4.1.1 与海南省一体化在线政务服务平台对接

实现与海南省一体化在线政务服务平台对接，主要对接如下：

（一）海南公安便民惠企服务应用能够按照省一体化在线政务服务平台的标准要求，与一体化在线政务服务平台入口（移动端和 PC 端）的对接，实现公安便民惠企服务在一体化在线政务服务平台中办理；

（二）海南公安梳理的便民惠企服务事项清单，根据省一体化在线政务服务平台的要求进行对接，实现公安服务事项清单同步到省政务服务清单中；

（三）海南公安采集的便民惠企的数据按照标准，实时提供给省政务服务平台及省其他厅直单位调用；

（四）便民惠企的数据进入公安网后，汇聚到公安信息资源服务平台，按照和省政府信息资源服务平台数据对接标准，定时按需把数据共享到省政府信息资源服务平台，为民众办理其他民生事项提供数据共享服务。

2.4.1.2 与公安部互联网+政务服务平台对接

实现与公安部互联网+政务服务平台对接，主要对接如下：

（一）海南公安便民惠企服务应用能够按照公安部的标准要求，与公安部互联网+政务服务平台对接，实现公安便民惠企服务在公安部互联网+政务服务平台中办理；

（二）海南公安梳理的便民惠企服务事项清单，根据公安部互联网+政务服务平台的要求进行对接,实现公安服务事项清单同步到公安部政务服务清单中；

（三）实现公安部用户平台在海南省微警务平台用户认证，部级平台登录后可以直接在省级平台办理业务；

（四）实现海南省级民生业务数据上报到公安部。

2.4.1.3 与海南省政府网站集约化平台对接

在咨询建议业务系统中，需要把社会公众提交的咨询和建议业务与海南省政府网站集约化平台对接，web 端提交的建议会进行筛选主动推送到政务云服务器上（可以匹配政务云上的身份证），管理员的回复都会主动的推送给服务器上。

2.4.2利警服务应用方面

平台能够支持与现有移动警务应用对接，各业务警种根据业务需求，根据警务微信平台的统一接口规范标准，对现有的移动警务应用进行移动化改造，满足平台对接要求。

2.5 国密算法升级

公安身份认证与访问控制管理系统（简称 PKI 系统）是公安信息系统的重要安全基础设施之一，系统主要包括 CA(签发中心)、RA（注册中心）、KMC（密

钥中心)、LDAP（目录服务）等模块，分别实现数字证书注册、证书签发、密钥管理、证书目录服务等功能，建设 PKI 系统能够解决公安信息化系统应用中的用户管理、身份认证、应用授权和责任认定等方面的问题，实现信息资源跨地区、跨部门的安全共享和高效应用。

根据公安部 2015 年下发的《公安机关信息化国产密码应用规划(2016-2020年)》、2016 年下发的《全国公安移动警务建设总体技术方案(2016)版》、《新一代公安移动警务 PKI 系统建设方案》和 2017 年下发的《关于印发<全国公安身份认证与访问控制管理系统国产密码算法替换建设任务书>》，明确了公安部 PKI 系统的顶层设计和规划：省级公安机关分别在公安信息网和公安移动信息网内建设用于警员和协辅警的数字证书签发和管理。同时根据公安部《公安信息网重要应用系统单轨制改造任务书》要求，所有在公安信息网上运行的重要信息系统必须实现基于数字证书的认证和授权。

对公安信息网警员 PKI 系统进行国产化密码算法升级，另需建设公安信息网辅警、移动警务二套 PKI 系统，依托公安部根 CA,合理规划和复用硬件资源，构建全省公安 PKI 系统的统一架构、统一标准、统一管理和跨网互认体系，使警员和辅警在公安信息网和移动警务内实现基于数字证书资源访问行为的实名制审计，有效提升新时期警务业务的安全保障能力。

3 项目实施需求

3.1 部省互联互通

海南省公安厅智慧微警务平台需要与公安部移动警务平台实现互联互通，包括集中管控互联、即时通讯软件互联等。

3.2 市县建设规划

各市县公安局统一使用省公安厅建设的海南公安“智慧微警务”项目平台，不再独立建设，接入海南公安“智慧微警务”项目平台规划如下：

一、建设海南公安“智慧微警务”项目应用

各市县公安局可根据本地的实际情况建设海南公安“智慧微警务”项目应用，包括便民惠企服务应用和利警服务应用。建设应用时需向省公安厅申请，通过省公安厅批准后才能进行建设，应用所需的资源（I 类、II 类、III 类）统一由省公安厅提供。

二、提供移动警务终端接入点

为市县提供省公安厅 APN/VPDN 接入点,满足不同场景业务需求的手持式和便携式移动警务终端装备。市县公安局根据自身实际情况，自行配备新一代移动警务终端。

三、技术要求

智慧微警务建设应符合《全国公安移动警务建设总体技术方案(2016 版)》、《移动警务视频安全接入规范》(公科信〔2013〕139 号)、《移动警务 B/S 应用安全接入规范》(公科信〔2010〕130 号)、《公安信息移动接入及应用系统建设技术指导书》(公信通〔2006〕541）等相关标准规范要求。市县建设应遵循以下技术要求：

（1）移动警务应用技术要求

1）基础共性应用

在省级应用开发组件的基础上，根据本地需要扩展标准应用监测和应用开发组件，建设适合本地业务情况的基础共性应用。

2）专业移动应用

实现包括移动视频调阅、PGIS、指挥调度等在内的移动综合应用；开展地方交管、出入境、刑侦、治安类等公安专业应用，开发警务公开、便民服务、警民互动等移动互联网应用。

（2）移动警务终端技术要求

支持终端密码模块运行，具备如指纹识别、人像识别等人机认证功能，通过安装终端安全监控组件，实现部分外设管理、终端监测、终端控制和终端审计等安全功能。优先选用具备国产化核心部件、国产化操作系统、符合我国可信计算设计的移动警务终端。

1）增强受控终端

支持采用内核可信增强、访问控制、网络控制、外设控制、应用控制、位置控制、可信安全保密等措施，实现防 root、防刷机、数据防泄漏、强制访问控制、安全漏洞远程修复、存储数据加密等安全功能，与安全相关的核心代码必须自主可控。

优先选用具备国产化核心部件、国产化操作系统、符合我国可信计算设计的移动警务终端。

支持终端密码模块运行，具备如指纹识别、人像识别等人机认证功能，通过预装终端安全监控组件，实现外设管理、终端监测、终端控制和终端审计等安全功能。

2）一般受控终端

支持终端密码模块运行，具备如指纹识别、人像识别等人机认证功能，通过安装终端安全监控组件，实现部分外设管理、终端监测、终端控制和终端审计等安全功能。

优先选用具备国产化核心部件、国产化操作系统、符合我国可信计算设计的移动警务终端。

3）个人普通终端

由使用者自行管理，自身安全不做强制性要求。

3.3 实施周期

本项目建设周期为 12 个月。

	1	2	3	4	5	6	7	8	9	10	11	12
项目招投标												
方案设计												
基础支撑系统建设												
应用系统建设												
标准规范编制												

	1	2	3	4	5	6	7	8	9	10	11	12
人员培训								━	━			
系统初验试运行									━	━	━	
项目验收												━

表 9- 1 项目进度表

3.4 项目管理

根据项目建设单位内部职能划分，公安厅有关人员、承建单位共同组成本项目的建设实施机构——项目工作组，负责项目实施管理，定期召开工作例会。项目实施过程的重大问题向项目组进行汇报。

承建单位要严格进行项目管理，各阶段都应提交相应的计划、设计，并经项目工作组认可后方可进行下阶段工作;并应确保人力、物力的定量投入，定期向项目组提交项目进展情况报告。

3.5 培训要求

承建单位必须提供技术后援支持，为今后系统中系统软件提供长期的技术支持。技术支持的方式包括：原厂技术服务、电话技术服务、邮件技术支持、现场技术服务、定期巡查服务、技术升级服务等。**A 包供应商需负责统筹整个项目的集成，负责整个项目的培训费。**

本项目培训包括技术培训、维护培训、使用操作培训几部分，由项目使用主要产品研发厂商、项目管理专家、信息系统建设专家向用户提供培训。所有培训教员使用中文进行授课，所有培训资料由中文书写。

培训地点在海南省内指定地点，设备由用户负责提供，由产品研发厂商及相关专家负责提供培训教材、培训内容。

培训方式分为现场培训和集中培训两种。

现场培训针对操作任务，通过视频培训，使操作人员了解应用系统及设备的结构、工作原理，掌握正确使用与操作和排除一般故障的能力。

集中培训主要针对系统管理人员，系统组织 3 期业务培训，每期为期 5 天，每期培训按 70 人规划培训地点及食宿安排。通过培训，使系统管理员对各种应用系统软件的安装、配置、优化、管理有一定的了解，可以进行日常的系统维护工作。培训对象包括参与项目建设和系统运行维护的各类管理人员、专业技术人员和系统操作使用人员，分三个层面进行人员培训。

1、公安厅平台管理人员。

重点是培养 5 名平台管理人员。

2、公安厅平台操作人员。

为公安厅计划培养 100 名平台操作骨干。

3、县市平台操作人员。

在市县公安机关中选取 70 名既懂业务又能熟练运用计算机技术的骨干,作为市县操作人员进行培训。

3.6 安全服务

信息系统的安全性及信息系统的构成、应用情况、网络结构、安全现状加以分析研究，编制信息系统测评技术方案和实施方案，对信息系统开展信息安全等级保护测评。通过等级测评进一步完善信息系统安全管理和技术防护，切实提高信息系统安全防护能力。

突发事件应急演练以提高相关工作人员应对突发事件的综合水平和应急处置能力，以防范信息系统风险为目的，建立统一指挥、协调有序的应急管理机制和相关协调机制，以落实和完善应急预案为基础，全面加强信息系统应急管理工作，并制定有效的问责制度。

需要提供一次应急演练服务，至少为期 5 天。

3.7 运维服务

3.7.1日常售后服务

提供系统的全套完备的中文技术文件，包括系统说明书、安装手册、设备配置和操作维护说明书，与系统有关的其他技术文件。

提供免费的技术咨询、故障诊断、系统升级等热线服务，为用户提供及时、迅速、优质的服务。

日常支持可以通过电话、传真、电子邮件、网站等方式实现。具体如下：

电话支持：提供技术信息和诊断支持，并解决有关问题；

传真支持：通过传真方式提供诊断支持，并解决有关问题。

3.7.2应急售后服务

投标人需指定专人负责提供 7*24 小时的应急支持服务，10 分钟内电话响应；重大故障 1 小时内上报，4 小时内解决，12 小时内出具故障报告；普通故障 2 小时内上报，8 小时内解决，48 小时内出具故障报告。

3.7.3现场售后服务

针对用户不能排除故障的，承建商需提供现场应急服务。

3.7.4巡检售后服务

为了保证系统的正常运行，承建商需为项目提供每年定期巡检服务。

3.7.5售后服务期内的服务目标

本项目要求提供三年的售后服务,在免费维护期内如出现系统或产品故障，

投标人对其负责的系统和产品进行维护，不收取费用。同时，保证在第一时间内对科信部门所提出的维护要求做出技术响应。存储设备需要返厂维修时，不得将硬盘带出，保管好所有敏感信息，不得外泄。

3.7.6合同结束后的服务目标

在合同结束后，投标人需提供保修服务，此时将视系统整体情况收取一定的费用。同时，需保证在规定时间内对科信部门所提出的要求做出技术响应。

3.7.7联网服务

投标人须提供与公安部联网服务子平台互联互通的技术支撑服务。

3.8　售后服务

承建单位必须提供技术后援支持，为今后系统中系统软件提供长期的技术支持。技术支持的方式包括：原厂技术服务、电话技术服务、邮件技术支持、现场技术服务、定期巡查服务、技术升级服务等。

所有软件、硬件设备及产品均需提供三年（项目终验之日起）的免费质保期。质保期从项目通过终验之日起计算。

质保期内，所有硬件设备的维修、更换及系统软件的维护、升级及性能优化均为免费，硬盘须提供原介质不返还的保修服务（即硬盘在发生故障后，由原厂商用相同品质的硬盘替换，但原有硬芯不得带走，由用户自行处理）。

质保期内，所有设备维修服务、技术升级服务均为上门服务，由此产生的费用均不再收取。

自项目终验之日起,需提供不低于 10 个驻点技术支持人员至少三年的现场技术支持,对海南省公安厅进行系统的日常维护(包含软硬件、及各类资源库),技术人员需具备维护系统的技术能力和工作经验（至少 1 人具备中级工程师证

书），并经本项目采购单位认可，在采购人指定的办公地点工作，接采购人的监督和指导，从事系统日常维护和巡检工作。

系统承建商提供每周 7 天，每天 24 小时的售后服务，在接到用户故障报告后反应时间不多于 2 小时，修复时间不超过 12 小时。如有系统软件升级、系统故障，应免费进行。

系统承建商应提供书面的技术服务承诺，明确售后服务的服务方式、范围、内容及费用。

3.9 后期运营推广

海南公安“智慧微警务”项目用户群体主要分为：民众和民警。民众是面向社会所有人员，民警主要分为业务型领导、政工型领导、业务型骨干警员、富有资历的警员等用户群。各用户群的主要需求如下：

（一）民众

民众的需求在于办事，需要分析民众的办事流程，提升办事效率。

（二）民警

民警主要按以下类型用户来划分：

1、业务型领导：领导力、业务方向把控、重要工作推动情况、向上通达、选人用人；

2、政工型领导：党建工作、警营文化、评优评先、掌握警员思想动向、向上通达；

3、业务型骨干警员：业务推动情况、向上通达、党性修养；

4、富有资历的警员：身体健康情况、党性修养、业务推动。

根据项目具体应用设置，海南公安“智慧微警务”项目的推广应用应参考互联网产品运营思路，构建移动警务运营体系，激活各类用户的活跃率，真正打造出一个受用户喜爱的移动应用产品。

投标人需提供完整的项目运营推广方案，并进行成本核算。

注：运营部分费用不在本次项目招标范围。

3.10 智慧微警务验收测评

按照公安部《新一代公安移动警务平台的验收测评》文件要求，本项目移动警务验收测评需通过“安全功能测评、等级保护测评、密码测评”。

3.11 廉政及保密要求

系统集成商要与公安厅签署《项目承建单位廉政责任承诺书》，系统集成商及相关施工人员要与信息中心签署保密协议，工作内容和文档要求按保密工作相关规定进行管理。

3.12 提供项目实施配套设备

1、项目承建单位自行负责解决现场实施所需办公设备，包括现场实施所需要的 10 台移动笔记本电脑（Intel 酷睿 i7 8565U；内存 16GB LPDDR3（低功耗版）2133MHz;1TB SSD 固态硬盘;13.9 英寸屏幕尺寸;支持十点触控防指纹;NVIDIA Geforce MX250 性能级独立显卡；3000x2000 超高清屏屏幕分辨率）并严格按照入网管理专机专用，项目建设结束后，由采购方按照相关工作要求技术检测和处理，设备中无相关敏感信息存储内容后返还。

2、项目 A 包承建单位提供至少 10 台大数据移动应用功能测试所需警务通终端设备（支持全网通，双卡双待；支持移动/联通/电信 4G+/4G/3G/2G；运行内存 RAM≥8G；机身存储≥256G；电池容量≥4000mAh；前置摄像头≥2400 万像素；后置摄像头≥4000 万+2000 万+800 万像素；支持指纹识别），并严格按照入网管理专机专用，项目建设结束后，由采购方按照相关工作要求技术检测和处理，设备中无相关敏感信息存储内容后返还。

4 项目采购清单

4.1 项目软硬件设备及材料采购清单

序号	名 称	技术参数要求	单位	数量	备注
	一、移动互联网服务子平台				
（一）	**专用设备**				
1	网络探针	主要功能：采集公安内网所有设备的运行状态，包括 CPU、内存、网络等使用情况以及由操作系统产生的各类异常告警信息等；采集公安内网主要安全设备和业务系统的业务运行日志、管理员管理操作日志以及系统告警信息等；获取集中监管与审计系统、统一运维系统的管理参数，对公安内网网络设备的网络信息进行联动管理；支持与集中监管与审计系统的交互，获取对终端用户的管控策略；支持对采集的数据按照后台系统提供的规则进行数据清洗、抽取、分析，实现对用户流量、应用流量、应用访问频次的统计，并在此基础上对安全事件进行告警记录；支持与公安内网的统一运维系统对接，实现实时掌握设备状态，进行跨网版本升级、配置更新等统一维护操作； 协议支持：将通过 SYSLOG、v2/SNMP v3、Telnet、ICMP 等方式获取到的信息传输给内网集中监控管理系统；支持 SYSLOG、v2/SNMP v3、Telnet、ICMP 协议； 管理功能：使用基于 HTTPS 方式的管理设备； 稳定性运行时间(MTBF)：＞50000 小时； 网络接口：≥6 个千兆网络接口； 性能要求：吞吐量≥800Mbps；支持≥200 个采集单元。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。	台	1	
2	数据探针	功能要求：采集所在区域业务数据，按照过滤策略进行敏感数据报警、接收数据副本功能； 数据清理后进行上报集控中心。协议支持：SYSLOG、v2/SNMP v3、Telnet、ICMP； 管理功能：使用基于 HTTPS 方式的管理设备；	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		稳定性运行时间(MTBF)：＞50000 小时； 网络接口：≥6 个千兆网络接口； 性能要求：吞吐量≥800Mbps；支持≥200 个采集单元。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。			
3	安全管控系统	主要功能： 1）I 类区各要素数据采集。按照《移动警务安全管控接口规范 20180921》标准与移动互联网服务子平台内其他系统及网络设备对接，对接范围包括本区域应用支撑系统、主机服务器、网络设备、安全设备等。 2）I 类区数据分类处理。将采集的数据信息进行存储、分类预处理、归并和压缩等操作。 3）I 类区策略接收下发。接收集中管控中心控制策略，并下发到 I 类区管控指令执行系统和网络设备。 4）I 类区级联数据上报。将 I 类区分类处理后的格式数据上报集中管控中心。 部署要求：支持通用服务器部署； 性能要求：支持与≥200 个设备对接，支持与≥200 个应用系统对接；解析处理能力 ≥800 条每秒； 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。	台	1	
4	云服务密码机	硬件要求：支持串口或网络配置管理接口。打印接口：支持串行打印机或者并行打印机。密钥存储：采用安全芯片实现密钥的存储，保证密钥的安全。机架式 2U 高度；提供设备运行状态指示灯，至少能标识正常和故障状态；至少提供 2 个网络端口；随机提供机架安装套件。 密码算法：采用国家密码管理局批准的硬件芯片实现各类密码算法，保证算法的高安全性；对称算法：支持国产 SM1/SM4 算法、以用国际通用算法 DES、TDES、AES；摘要算法：支持国产 SM3 和通用 SHA1/SHA256/SHA384/SHA512 等算法；非对称算法：支持国产 SM2 和通用 RSA(1024-4096 位)算法。 性能要求：SM2 签名 ≥ 50000 次/秒；SM2 验签名 ≥ 15000 次/秒；SM1 加解密 ≥ 100 Mbps；SM3 摘	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		要≥ 500 Mbps；SM4 加解密≥ 500 Mbp。 密码产品资质要求：产品需具有国家密码管理局颁发的商用密码产品型号证书，并提供该产品商用密码产品型号证书复印件，并加盖原厂商公章。			
5	签名服务器	设备高度 设备高度 3U 物理参数 500*430*132 电源 电源 标配 2 个 550W 电源 工作电压 220~240V 接口标准 网口 1000M*2 工作环境 工作温度 0 ° C--45 ° C 相对湿度 5 %--95% RH，不凝结 性能参数 数字签名（国密算法） 12000 次/秒 签名验证（国密算法） 12000 次/秒	套	2	
（二）	数据迁移	提供数据迁移服务	套	1	
	二、联网服务子平台				
（一）	**计算资源**				
1	云管理节点	整机 机架式服务器，服务器高度≥2U，标配原厂导轨 CPU: ≥2 颗 Intel SP 4116，单颗核芯≥12 核,双线程，主频≥2.1GHz； 内存：≥64G DDR4 内存，频率≥2400MT，可扩展≥24 个内存插槽，最大支持最大容量 3.0TB 硬盘：≥8 个 2.5 寸热插拔硬盘槽位，≥ 6*600G 10K SAS，可扩展至≥40 个热插拔硬盘槽位，提供官网截图并加盖生产厂商项目授权章 网卡：≥2*10G SPF+ ，含模块；≥4*GE 电口； RAID 卡：≥1 个板载 专用插槽的 Raid 阵列卡，支持 Raid0/1/10/5，≥2GB 缓存，含断电保护	台	3	

序号	名　称	技术参数要求	单位	数量	备注
		最多提供≥10 个 PCIE3.0 插槽（其中可支持≥3 个全宽高性能 GPU 卡），提供官网截图并加盖生产厂商项目授权章。 电源：本次配置 2 个≥500w 热插拔冗余电源，1+1 冗余电源 管理 配置≥1Gb 的远程管理控制端口，配置虚拟 KVM 功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟媒体等操作，提供服务器健康日记、故障现场还原，支持智能电源管理，支持服务器内部温度切面的 3D 显示，可支持动态功率封顶。 产品资质 ▲产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过 QC 080000 有害物质过程管理体系认证，提供证书复印件，并加盖原厂商公章或投标专用章 ▲为保证本项目的完善实施、严格按照要求落地，制造厂商均须具备良好的商业信誉，提供国家企业信用信息公示系统（网址：http://www.gsxt.gov.cn/）上行政处罚信息一栏的网站截图（带完整 URL 链接）证明，在“行政处罚内容“栏目内无行政处罚记录，并加盖厂商项目授权章；			
2	警务微信接入服务器	整机 机架式服务器，服务器高度≥2U，标配原厂导轨 CPU: ≥2 颗 Intel SP 4116，单颗核芯≥12 核,双线程，主频≥2.1GHz； 内存：≥64G DDR4 内存，频率≥2400MT，可扩展≥24 个内存插槽，最大支持最大容量 3.0TB 硬盘：≥8 个 2.5 寸热插拔硬盘槽位，≥ 6*600G 10K SAS，可扩展至≥40 个热插拔硬盘槽位，提供官网截图并加盖生产厂商项目授权章 网卡：≥2*10G SPF+ ，含模块；≥4*GE 电口； RAID 卡：≥1 个板载 专用插槽的 Raid 阵列卡，支持 Raid0/1/10/5，≥2GB 缓存，含断电保护 最多提供≥10 个 PCIE3.0 插槽（其中可支持≥3 个全宽高性能 GPU 卡），提供官网截图并加盖生产厂商项目授权章。 电源：本次配置 2 个≥500w 热插拔冗余电源，1+1 冗余电源 管理 配置≥1Gb 的远程管理控制端口，配置虚拟 KVM 功能，可实现与操作系统无关的远程对服务器的完	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟媒体等操作，提供服务器健康日记、故障现场还原，支持智能电源管理，支持服务器内部温度切面的 3D 显示，可支持动态功率封顶。 产品资质 ▲产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过 QC 080000 有害物质过程管理体系认证，提供证书复印件，并加盖原厂商公章或投标专用章 ▲为保证本项目的完善实施、严格按照要求落地，制造厂商均须具备良好的商业信誉，提供国家企业信用信息公示系统（网址：http://www.gsxt.gov.cn/）上行政处罚信息一栏的网站截图（带完整 URL 链接）证明，在“行政处罚内容“栏目内无行政处罚记录，并加盖厂商项目授权章；			
3	警务微信存储服务器	整机 机架式服务器，服务器高度≥2U，标配原厂导轨 CPU: ≥2 颗 Intel SP 4116，单颗核芯≥12 核,双线程，主频≥2.1GHz； 内存：≥64G DDR4 内存，频率≥2400MT，可扩展≥24 个内存插槽，最大支持最大容量 3.0TB 硬盘：≥8 个 2.5 寸热插拔硬盘槽位，≥ 6*3.8T SSD，可扩展至≥40 个热插拔硬盘槽位，提供官网截图并加盖生产厂商项目授权章 网卡：≥2*10G SPF+ ，含模块；≥4*GE 电口； RAID 卡：≥1 个板载 专用插槽的 Raid 阵列卡，支持 Raid0/1/10/5，≥2GB 缓存，含断电保护 最多提供≥10 个 PCIE3.0 插槽（其中可支持≥3 个全宽高性能 GPU 卡），提供官网截图并加盖生产厂商项目授权章。 电源：本次配置 2 个≥500w 热插拔冗余电源，1+1 冗余电源 管理 配置≥1Gb 的远程管理控制端口,配置虚拟 KVM 功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟媒体等操作，提供服务器健康日记、故障现场还原，支持智能电源管理，支持服务器内部温度切面的 3D 显示，可支持动态功率封顶。 产品资质 ▲产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过 QC 080000 有害物质过程管理体系认证，提供证书复	台	3	

序号	名　称	技术参数要求	单位	数量	备注
		印件，并加盖原厂商公章或投标专用章 ▲为保证本项目的完善实施、严格按照要求落地，制造厂商均须具备良好的商业信誉，提供国家企业信用信息公示系统（网址：http://www.gsxt.gov.cn/）上行政处罚信息一栏的网站截图（带完整 URL 链接）证明，在“行政处罚内容“栏目内无行政处罚记录，并加盖厂商项目授权章；			
4	云计算节点	整机 机架式服务器，服务器高度≥2U，标配原厂导轨 CPU: ≥2 颗 Intel SP 6132，单颗核芯≥14 核,双线程，主频≥2.6GHz； 内存：≥256G DDR4 内存，频率≥2400MT，可扩展≥24 个内存插槽，最大支持最大容量 3.0TB 硬盘：≥8 个 2.5 寸热插拔硬盘槽位，≥ 2*600G 10K SAS，可扩展至≥40 个热插拔硬盘槽位，提供官网截图并加盖生产厂商项目授权章 网卡：≥2*10G SPF+ ，含模块；≥4*GE 电口； RAID 卡：≥1 个板载 专用插槽的 Raid 阵列卡，支持 Raid0/1/10/5，≥2GB 缓存，含断电保护 最多提供≥10 个 PCIE3.0 插槽（其中可支持≥3 个全宽高性能 GPU 卡），提供官网截图并加盖生产厂商项目授权章。 电源：本次配置 2 个≥500w 热插拔冗余电源，1+1 冗余电源 管理 配置≥1Gb 的远程管理控制端口，配置虚拟 KVM 功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟媒体等操作，提供服务器健康日记、故障现场还原，支持智能电源管理，支持服务器内部温度切面的 3D 显示，可支持动态功率封顶。 产品资质 ▲产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过 QC 080000 有害物质过程管理体系认证，提供证书复印件，并加盖原厂商公章或投标专用章 ▲为保证本项目的完善实施、严格按照要求落地，制造厂商均须具备良好的商业信誉，提供国家企业信用信息公示系统（网址：http://www.gsxt.gov.cn/）上行政处罚信息一栏的网站截图（带完整 URL 链接）证明，在“行政处罚内容“栏目内无行政处罚记录，并加盖厂商项目授权章；	台	30	

序号	名　称	技术参数要求	单位	数量	备注
（二）	**存储资源**				
1	数据存储	整机 ▲多控制器架构，控制器之间采用 PCI-E 或 Infiniband 对等高速总线的全网状互连，多个控制器可以并行读写配置 4 个存储控制器，每个控制器之间通过 PCI-E 或 Infiniband 高速总线点对点对等互联，需提供厂商官网截图证明并加盖原厂项目授权章 ▲每个控制器配置 2 颗存储处理芯片，需提供厂商官网截图证明并加盖原厂项目授权章，控制指令和数据的传输通道物理分离，主控芯片也同样物理分离 配置 16Gbps FC 主机端口≥8 个，10Gb iSCSI 主机端口≥8 个 配置高速缓存≥128GB，缓存不包含 SSD 磁盘、PCI-E SSD、闪存、压缩或重删缓存和 NAS 控制器缓存 配置≥16 块 2.5″400GB SSD 企业级硬盘，≥16 块 2.5″1.8TB 10K SAS 企业级硬盘，≥36 块 8T 7.2K SAS 企业级硬盘 所有磁盘可同时配置为 RAID0/1/5/6，且可共存，支持无中断地 RAID 改变，支持多类型磁盘多方向、无中断在线数据迁移，迁移过程不影响业务性能 采用高速多对多磁盘故障恢复方式，提高恢复速度的同时，可保证磁盘复期间应用的性能，无专用指定热备盘，重建全局并发 配置硬盘扩展柜保护功能，当配置多个硬盘扩展柜时，可支持至少一个硬盘扩展柜掉电或故障时数据不丢失，应用不中断 存储功能 支持基于控制器的 SAN+NAS 软件授权，支持原生的 NAS 功能，无需另配 NAS 网关从主机端口到硬盘全路径支持基于硬件的并符合业界标准的 T10-PI 数据一致性检测，保障数据的一致性，需提供厂商官网截图证明并加盖原厂项目授权章 配置图形界面管理软件，支持多种语言（至少包括简体中文和英文），支持多台设备集中管理，支持存储资源管理分析和资源使用历史记录分析，支持 WEB 管理，支持 CLI 管理。支持多种事件通知功能 配置自动精简、克隆、QoS、重删压缩、自动分层 配置性能监控和分析软件，配置高级图形化报表软件，可以定制历史运行数据的图形化报表	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		支持将快照直接备份到二级存储或者服务器上，支持二级存储/服务器上所备份的快照恢复到原磁盘阵列或其他磁盘阵列 支持存储远程复制功能，支持与同厂商高端型号以及全闪存阵列间实现存储底层复制，包括远程复制和可在线迁移卷 支持存储双活功能，在不加额外网关的情况下可以实现和同厂商高中端型号存储组成双活阵列，在一台阵列故障的情况下，主机 IO 访问可以无缝切换到另外一台阵列而不会中断业务 在不加额外网关的情况下可以实现和同厂商的高中端存储和全闪存存储组成存储集群，数据可以在多台存储之间按照性能、容量等策略进行在线数据迁移，对于主机平台透明 产品资质 投标产品必须为成熟产品，并需提供官方 6 个 9 的高可用证明并盖原厂项目授权章			
2	备份存储	整机 要求与存储设备同品牌；可与现有的备份应用和流程实现无缝集成，专用磁盘备份设备，非虚拟带库网关架构 配置处理器≥2 颗，≥8 核 配置高速缓存≥128GB 配置≥4 个 10Gb 以太网接口 配置≥12 块 4TB 7200 转 SAS 硬盘，备份可用的数据磁盘存储可用容量≥31.5TB，最大扩展可用容量可达 108TB 采用 RAID 6 保护；支持热插拔硬盘、冗余电源、风扇等 单台设备可虚拟的磁带库及 NAS 数量≥36 支持模拟的磁带格式为 LTO-4、LTO-5，LTO-6 和 LTO-7 等 备份目标方式 支持 NAS、VTL 和 Symantec OST 三种备份目标方式 NAS 备份目标要求支持 NFS 和 CIFS 要求 iSCSI 环境下支持 VTL 备份目标方式 本次要求配置 VTL,NFS,CIFS,OST 功能	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		存储功能 提供在线重复数据删除技术，提供磁盘备份设备之间的低带宽数据复制许可 采用可变长数据块重复数据删除，提高重复数据删除效率 配置无限容量许可的中文图形化虚拟带库管理软件，可以通过一个管理软件管理多台虚拟带库设备 支持将备份设备直接作为 Oracle RMAN 目标进行 Oracle 备份 支持将备具备自动管理、自动配置、自动监控及性能调试等功能，可通过简单的界面进行轻松安装份设备直接作为 SQL 目标进行 SQL 备份 支持将备份设备直接作为 Exchange 目标进行 Exchange 备份 支持并包含将主阵列的快照备份到本设备，并且将快照恢复到原始阵列或者其他相同快照格式阵列			
（三）	**网络资源**				
1	核心交换机	整机 框式交换机，采用正交 CLOS 架构，能够配置独立的交换网板，业务线卡槽位与交换网板槽位互相垂直，提供官网证明和实物正反面图片，指明槽位物理位置关系，并加盖原厂项目授权章 业务插槽数量≥6，主控引擎模块≥2,交换网板≥1 交换容量 ≥ 30 Tbps，包转发率≥5500Mpps 实配万兆光口≥24 个，含堆叠模块，配置 20 个万兆多模光模块(850nm,300m,LC) 和 4 个千兆多模光模块(850nm,0.55km,LC) 为符合未来网络速率和端口密度的发展以及板卡扩容，单槽位 10G 端口密度≥48 个，单槽位 40G 端口密度≥32 个，单槽位 100G 端口密度≥16，提供官网截图链接，并加盖原厂项目授权章，业务板均要线速转发 支持多种业务板卡扩展，支持 FW、IPS、NSM、上网行为管理、负载均衡、SSL VPN 等安全独立硬件板卡，提供官网截图链接，并加盖原厂项目授权章 支持 RPR 接口 支持将 N 台物料设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合，支持 4 框虚拟化技术，提供第三方权威权威检验报告，并加盖原厂项目授权章	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		功能 支持 OPENFLOW 1.3 标准，支持多控制器（EQUAL 模式、主备模式），支持多表流水线，支持 Group table，支持 Meter 支持 VxLAN 功能，提供官网配置手册截图和链接，并加盖原厂项目授权章 支持跨数据中心的二层互联技术，各数据中心各节点可以实现二层互通，数据中心内虚拟机可在数据中心间可自有迁移，用户网络和服务提供商网络无需做任何变动 支持 FCOE 等数据中心特性，提供第三方权威权威检验报告，并加盖原厂项目授权章 支持主流的 MAC in IP 技术，如 EVI/EVN/OTV 等，实现跨三层网络的二层互联，提供官网配置手册截图和链接,并加盖原厂项目授权章 支持基于端口的 VLAN，802.1q Vlan 封装，最大 Vlan 数>=4096，支持 GVRP ； 支持优先级队列，支持 SP、WRR、SP+WRR 队列调度算法 支持 PIM-DM、PIM-SM、PIM-SSM、MSDP、MBGP 、Any-RP、IGMPv1/v2/v3 等协议，支持 PIM6-DM、PIM6-SM、MLDv1 等协议 支持 IPv4 和 IPv6 双协议栈，支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+，支持 IPv4 向 IPv6 的过渡技术，包括：IPv6 手工隧道、6to4 隧道、ISATAP 隧道、GRE 隧道、IPv4 兼容自动配置隧道等 支持基于标准、扩展、VLAN 的 ACL 报文过滤，支持 OSPF、RIPv2 及 BGPv4 报文的明文及 MD5 密文认证 产品资质 ▲为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；			
2	云平台数据交换机	整机 固化千兆以太网电接口≥48，上行万兆光接口数量≥4，满配业务扩展槽≥1，模块化双电源、模块化双风扇，配置 2 个万兆模块，含堆叠模块，配置可插拔防火墙硬件板卡一块 交换容量 ≥ 590 Gbps，包转发率≥250Mpps 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN 等功能，需提供官网选配信息截	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		图证明，并加盖原厂项目授权章 功能 支持基于端口的 VLAN、基于 MAC 的 VLAN 支持 IPv4 静态路由、RIP V1/V2、OSPFv1/v2、OSPFv3、BGP4，BGP4+ for IPv6 支持基于协议 VLAN 支持通过 SFP 端口进行堆叠，最多支持 9 台设备堆叠； 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms； 支持 DHCP Snooping，防止欺骗的 DHCP 服务器 支持 ARP 检测来抵御 ARP 欺骗攻击； 产品资质 ▲为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；			
3	云平台管理交换机	整机 固化千兆以太网电接口≥48，上行万兆光接口数量≥4，满配业务扩展槽≥1，模块化双电源、模块化双风扇，配置 2 个万兆模块，含堆叠模块，配置可插拔防火墙硬件板卡一块 交换容量 ≥ 590 Gbps，包转发率≥250Mpps 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN 等功能，需提供官网选配信息截图证明，并加盖原厂项目授权章 功能 支持基于端口的 VLAN、基于 MAC 的 VLAN 支持 IPv4 静态路由、RIP V1/V2、OSPFv1/v2、OSPFv3、BGP4，BGP4+ for IPv6 支持基于协议 VLAN 支持通过 SFP 端口进行堆叠，最多支持 9 台设备堆叠； 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms； 支持 DHCP Snooping，防止欺骗的 DHCP 服务器 支持 ARP 检测来抵御 ARP 欺骗攻击；	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		产品资质 ▲为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；			
4	存储交换机	整机 交换容量 ≥ 2.5 Tbps，包转发率≥1000Mpps 本次实配万兆光口≥48 个，40GE 光口≥2 个，业务扩展槽≥2 个，配置 48 个万兆多模光模块(850nm,300m,LC) 配置冗余双电源、冗余双风扇框，需提供官网截图和实物图片证明，并加盖原厂项目授权章 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN、LB 等功能，需提供官网选配信息截图证明，并加盖原厂项目授权章，本次配置可插拔防火墙硬件板卡一块 功能 支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换 支持静态路由、RIP v1/2、OSPF、BGP 等动态路由协议，支持 RIPng、OSPF V3、IS-IS V6、BGP+ FOR IPV6、IPV6 策略路由，支持 VRRP，支持等价路由支持基于端口的 VLAN、基于 MAC 的 VLAN 支持 VxLAN 集中式网关互通功能，支持 EVPN 分布式网关二三层互通功能 支持设备堆叠，最多支持 9 台设备堆叠 支持基于端口的 VLAN，支持基于协议的 VLAN 支持 IGMP v1/v2/v3，MLD v1/v2，支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2 支持 VRRPv2/v3（虚拟路由冗余协议），支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 200ms 产品资质 为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；	台	2	
5	控制区接入交换机	整机 固化千兆以太网电接口≥48，上行万兆光接口数量≥4，满配业务扩展槽≥1，模块化双电源、模块化双风扇，配置 2 个万兆模块，含堆叠模块，配置可插拔防火墙硬件板卡一块	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		交换容量 ≥ 590 Gbps，包转发率≥250Mpps 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN 等功能，需提供官网选配信息截图证明，并加盖原厂项目授权章 功能 支持基于端口的 VLAN、基于 MAC 的 VLAN 支持 IPv4 静态路由、RIP V1/V2、OSPFv1/v2、OSPFv3、BGP4，BGP4+ for IPv6 支持基于协议 VLAN 支持通过 SFP 端口进行堆叠，最多支持 9 台设备堆叠； 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms； 支持 DHCP Snooping，防止欺骗的 DHCP 服务器 支持 ARP 检测来抵御 ARP 欺骗攻击； 产品资质 为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；			
6	安全区域接入交换机	整机 固化千兆以太网电接口≥48，上行万兆光接口数量≥4，满配业务扩展槽≥1，模块化双电源、模块化双风扇，配置 2 个万兆模块，含堆叠模块，配置可插拔防火墙硬件板卡一块 交换容量 ≥ 590 Gbps，包转发率≥250Mpps 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN 等功能，需提供官网选配信息截图证明，并加盖原厂项目授权章 功能 支持基于端口的 VLAN、基于 MAC 的 VLAN 支持 IPv4 静态路由、RIP V1/V2、OSPFv1/v2、OSPFv3、BGP4，BGP4+ for IPv6 支持基于协议 VLAN 支持通过 SFP 端口进行堆叠，最多支持 9 台设备堆叠；	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms； 支持 DHCP Snooping，防止欺骗的 DHCP 服务器 支持 ARP 检测来抵御 ARP 欺骗攻击； 产品资质 为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；			
（四）	**软件**				
1	云资源管理平台	知识产权要求 ▲1、国产云计算平台软件，基于业界主流的开源云计算架构 OpenStack，厂商须掌握软件自主知识产权，并提供软件著作权证书。 产品成熟度 1、产品不仅能够帮助用户构建私有云，同时拥有公有云平台的运营。云平台可以同时管理私有云和公有云。 2、云平台需具备大规模资源的调度能力，厂商使用云计算平台技术，运营私有云业务或公有云两年以上，单个云平台节点规模不低于 800 台，其中单集群超过 500 台。 计算虚拟化 1、提供基于开源 KVM 的虚拟化引擎，并支持 VMWare 虚拟化，具备创建、修改、查询、删除虚拟服务器，以及调整服务器配置的能力。应支持通过虚拟机将物理计算资源“一虚多”，形成计算资源池；虚拟机应支持多种操作系统和版本；虚拟机之间相互独立，互不影响；应支持虚拟机系统自动批量部署。 2、支持将当前运行的虚拟服务器打包为模板，并通过自定义模板批量快速生成虚拟服务器的能力。支持虚拟机秒级快速部署，具备大规模部署特性的同时具备良好的性能保障，满足大规模资源快速创建的需求。 3、除了通过 IP 地址远程访问外，还支持通过浏览器界面直接访问和管理虚拟机，能够查看虚拟机的启动、运行、关机等整个生命周期状态。 4、云平台中无单独的共享存储设备（SAN 和 NAS）时，支持虚拟机在线或者离线迁移到指定物理节点，	套	66	

序号	名　称	技术参数要求	单位	数量	备注
		在线迁移过程中虚拟机业务不中断。 ▲5、支持主流 X86 服务器统一纳管调度，无需指定服务器品牌、型号。 6、支持虚拟机的高可用调度，支持对宿主机的指标进行多维度监控，并根据配置策略判断宿主机健康状况，对虚拟机进行自动化的高可用调度。 7、支持 GPU 池化功能，支持通过容器服务提供 GPU 容器，能够满足 GPU 应用场景的计算需求。 基于 OpenStack 的云计算管理平台 云计算管理平台最重要的两个特质在于管理云资源和提供云服务。即通过构建基础架构资源池（IaaS）、搭建企业级应用/开发/数据平台（PaaS），以及通过 SOA 架构整合服务（SaaS）来实现全服务周期的一站式服务，构建多层级、全方位的云资源管理体系。 在 IaaS 云中，云计算管理平台需要在虚拟化、网格计算、效用计算、分布式等技术的支撑下，对包括计算资源、存储资源、网络资源等在内的基础架构通过 API 接口进行管理，实现按需的、可计量的对基础架构资源进行分配，同时，实现对资源使用情况和健康情况的监控以及对事件的捕获和处理。 在 PaaS 云中，云计算管理平台应该可以通过抽象管理来将用户需求翻译成平台相关属性需求，通过平台管理和接口 API 编程来实现针对平台需求的资源切割和快速部署，并同样需要在此过程中实现平台资源的计量、监控，以及事件的捕获和处理。 在 SaaS 云层面中，云计算管理平台也需对实际业务需求进行抽象处理，形成应用服务管理的通用架构。要构建这样的通用架构中，还需云计算管理平台实现基于 SOA 服务的注册、注销、配置、流程设计、调度以及服务的部署等管理功能，同时在此过程中还需对服务质量和性能进行监控，并以此为依据进行服务级别（SLA）和服务计量的管理。 此外，云计算管理平台还需要面向用户和面向管理的统一门户来改善管理效率和提高用户体验。同时，在云计算管理平台的设计中，应考虑使用面向整个云计算管理平台的数据库，使所有的管理操作、用户使用情况、性能、事件等可回溯，同时可以此为基础进行数据分析、行为分析和决策支持，以提高整个云体系架构的服务水平和资源利用率。			

序号	名　称	技术参数要求	单位	数量	备注
		存储虚拟化 1、提供多种虚拟化存储服务：虚拟化存储服务提供块存储服务以及对象存储等统一存储功能。对象存储满足超大型文件的存储需求。 2、虚拟化存储产品基于 SAS 磁盘即可提供高性能保证，满足数据库、中间件等产品的性能需求，降低硬件采购成本。 3、使用 SAS 盘前提下，小文件每秒随机读操作次数（IOPS）达到主流水平，以保障数据库（如：ORACLE、DB2）在高压力下的正常运行。 4、在使用 SAS 盘前提下，虚拟存储设备小文件顺序写 IO 吞吐达到主流水平。 5、支持对磁盘总容量的实时监控，支持对虚拟存储的性能实施监控并设置告警阈值，当性能出现下降时或异常，能够立即告警。 6、支持纠删码技术，能够在节约硬件成本的同时保证数据存储的性能和可靠性。 网络虚拟化 1、支持完全基于软件实现的网络虚拟化功能，无须采购专有网络设备，无需绑定网络硬件，不使用有 SDN 功能的交换机。 2、支持基于软硬件结合的网络虚拟化功能，可以屏蔽底层不同 SDN 控制器厂商的差异。 3、分布式虚拟路由器，需支持网状网络（mesh network），在 VPC 内部的所有网段内部的主机之间的连接可以是网状连接，而非传统的树状连接，能够降低了跨网段导致的网络延迟和损耗。同时也需支持树状网络。 4、网络类型包含基础网络、受管私有网络、自管私有网络。支持指定虚拟主机的 IP 网络地址，可以设置静态 IP，支持外部 IP 资源分配与持久绑定。 5、提供虚拟三层设备的功能，支持 DHCP，端口转发， VPN，访问控制功能。 6、平台内部的虚拟主机可以与外部的其它系统通过三层网络进行各类应用层交互。包括但不限于双向			

序号	名　称	技术参数要求	单位	数量	备注
		的 HTTP 交互，FTP 交互，SSH 交互，数据库连接，RPC 调用。 云计算功能要求 1、云平台软件结构完整，通过统一架构和技术平台，实现服务器虚拟化、分布式存储和网络虚拟化等技术，为云服务提供可度量的、相对隔离的、安全的、快速可扩展的持续资源供给。 2、云平台软件不依赖特定的硬件，兼容管理主流的虚拟化系统，如 VMware vSphere、KVM 等。 3、云主机服务:像传统物理机一样，云主机可以添加或删除网卡、硬盘，更改主机 CPU/内存等。通过云平台提供一种随时获取的、弹性可扩展的计算能力，包括映像或主机实例。 4、容器技术支持：支持 Docker 容器技术。 5、云平台可同时支持分布式存储和 SAN 存储，在创建虚拟机或存储卷时，用户可以选择是使用分布式存储还是 SAN 存储。 6、对象存储服务：提供可无限扩展的存储空间、快速的数据存取性能、高度的可靠性和数据的安全性、细粒度的权限控制及简单易用的接口，以向用户提供廉价、可靠的存储系统。支持通过 http 方式进行下载。应采用多管理节点设计，避免集群单点失效，自动进行故障监测和数据迁移；应具备高可扩展性，可支持上亿个文件和 PB 以上量级的文件存储； 7、负载均衡：提供完全基于软件的负载均衡器功能，同时支持 TCP/HTTP/HTTPS 等协议，构建高可用的应用负载集群，降低购买硬件设备的支出和管理复杂度。 8、弹性伸缩：用户可根据自身业务需求，配置相应的告警策略，自动化进行服务器角色伸缩。 9、软件自动部署功能：用户可在创建虚拟机过程中，自助选择所需要的各类软件，如数据库（Oracle、MySQL 等）、中间件（Tomcat、WebLogic）等，云平台可以自动创建虚拟机，满足标准化运维的需求。 10、云资源编排：通过脚本化的方式调用、组合云平台提供的服务功能以达到自动化、标准化运维的目的。允许通过标准脚本方式快速创建一系列资源如虚拟机、存储、负载均衡等。并且支持在虚拟机中自动部署应用系统软件，当脚本中某个环节失败，则保证资源全部退回。 11、应用管理：提供业务可视化界面，快速查看当前云平台中部署的应用系统的情况，针对某一应用，还能查看该应用的所有相关信息，例如应用版本号、部署架构、占用虚拟机数量、应用组件关联关系、			

序号	名　称	技术参数要求	单位	数量	备注
		访问端口、应用负责人、进程监控、业务特性（在线用户数）监控等信息。 12、多资源调度策略支持：云平台能够按照业务需要划分服务器集群，如虚拟化集群、容器集群、对象存储服务集群等，不同集群资源使用策略会有所不同。云平台在创建虚拟机资源时无需指定具体在哪台物理服务器中，而是由云平台可定制的策略设置自动将虚拟机调度到最合适的服务器集群上进行承载。 13、云平台可支持计算节点动态扩展，当云平台资源不足时，新的物理服务器资源可自动识别，并加入到云平台资源池中，整个过程不会对原有服务造成影响。 14、提供裸金属服务，云平台可分配物理服务器，并进行操作系统的自动化部署 安全性 1、具备用户管理与用户隔离功能，确保用户间数据隔离与私密性。 2、可以通过软件定义网络 SDN 技术创建私有网络，私有网络间在二层 100%隔离，私有网络数量没有规模限制，增强二层网络的安全性及规模化应用，非使用 VLAN 技术控制广播。 3、支持 VPN 支持，提供软件防火墙等、SSH 等安全机制，帮助用户防护非授权访问与攻击。 4、虚拟网络支持 ARP 多路径决策功能，防止大量 ARP 广播造成的泛洪问题。 5、虚拟网络设备需提供自定义安全组策略。 6、提供资源备份功能。 7、支持资源回收站功能，支持误删除资源找回，提供操作安全保证。 8、支持针对租户的虚拟化安全产品，虚拟防火墙、虚拟 WEB 防护（WAF）、虚拟 IPS 等。 9、提供国内外普遍认可的安全认证证书说明，证明云平台及相关系统达到一定的安全标准。 高可用 1、基础云平台本身支持容灾架构，任意云管理控制器器宕机，云平台亦能正常运行，正在创建的虚拟机也能继续创建完成。 2、云平台中无单独的共享存储设备（SAN 和 NAS）时，当虚拟机所在物理服务器发生故障时，能够自动在其它物理服务器重新启动虚拟机，以尽快恢复业务的运行。 3、云平台网络控制器支持分布式部署架构，在任意管理控制节点出现故障时，云平台网络仍然能够正常工作，不影响业务运行。			

序号	名　称	技术参数要求	单位	数量	备注
		4、云平台存储控制器支持冗余架构，任一存储控制器出现宕机故障时，不影响云存储业务的运行；同时，云存储数据切片冗余保存多份，存储节点出现故障时，数据不丢失且不影响上层业务正常运行。 易用性 1、操作界面要充分考虑操作易用性，适合运维人员日常操作习惯，为用户提供图形化向导界面。 2、提供完善易用的 RESTful API 接口及文档，对云内所有资源及功能（如：主机、硬盘、网络、负载均衡器、防火墙、弹性 IP、监控等）提供 API 级别的支持。 3、支持云内资源的网络拓扑图展示功能，直观展现网络结构。 PaaS 功能支持 1、产品包含 PaaS 服务能力，提供集成的关系型数据库提升开发与测试效率。 2、提供高性能的关系型数据库服务，支持 MySQL、MSSQL 等多重数据库引擎，提供包括单机部署、主从部署或高可用架构等各种管理功能。 3、提供金融级分布式关系型数据库服务，兼容 MySQL 协议语法，具备多种类型的分区支持，分布式的架构可支持平行扩展，性能与容量线性增长。 4、提供云化 Oracle 功能，支持单机、高可用等多种部署模式，优化过的存储集群、计算集群为 Oracle 应用提供卓越的 TPM/IOPS 性能。 SaaS 功能支持 1、产品包含 SaaS 服务能力，通过接入多种 SaaS 生态服务，提升平台整体的应用效率。 2、提供 SaaS 源码管理平台服务，支持在本地管理源代码版本库，支持实时异地备份。 售后保障支持服务 提供产品原厂产品使用培训服务； 厂商可提供响应服务时间≦2 小时的故障分析和恢复； 为保证项目运营平台质量，需云平台原厂提供本项目实施服务；配合应用系统上云迁移，提供原厂 2 年 7X24 小时技术支持服务； 提供一名工程师驻场服务 1 年。针对以上服务需求，需出具原厂服务承诺函。 售后及实施服务要求 提供 7×24 小时电话支持及两小时上门服务。提供厂商针对本项目的原厂授权函与原厂售后服务承诺函。 对于因产品本身质量原因导致的重大故障，需保证一小时内恢复业务			

序号	名　称	技术参数要求	单位	数量	备注
		原厂 3 年维保服务，提供原厂工程师现场实施方案规划、部署、调优、巡检和培训服务。保修期内提供文档知识库、邮件支持、季度巡检以及升级软件版本服务。 要求产品需为投标人自有产品，须掌握软件自主知识产权，并提供软件著作权证书。 ▲投标人所投云计算平台产品需为知名厂商产品。国产云计算平台软件，基于业界主流的开源云计算架构 OpenStack，所投产品厂家具备 OpenStack 社区黄金以上会员资格，提供 OpenStack 官网（www.openstack.org）资助证明、软件著作权证书，加盖原厂商公章。			
	云服务自助平台	知识产权要求 1、与云资源管理平台软件为同一品牌，能够实现与云资源管理软件的无缝对接。厂商须掌握软件自主知识产权，并提供软件著作权证书。 部门与用户管理 1、支持部门组织架构管理功能，能够新增、修改部门信息，支持设置部门管理员。 2、支持部门用户管理，管理员可定义用户的不同角色，通过角色管理来控制用户的权限。 3、提供子用户功能，管理员可对子用户进行管理，进行新建、修改、禁用、密码重置和删除等操作。 4、提供项目管理功能，支持将不同部门的用户按照项目组织在一起。 5、用户登录平台后，只能看到自己或团队权限范围内的云资源。 资源服务目录 1、提供云平台资源服务目录，服务目录需包含弹性计算、弹性存储、负载均衡、主流数据库常用云服务 2、支持平台管理员在服务目录中发布新的服务，或对已有的服务进行配置、下架处理等。 资源配额管理 1、支持为平台用户分配一定的资源配额，用户在配额范围内可自助使用云平台的各种资源。 云资源使用与管理 1、平台支持接入多个独立的云资源池，支持使用同一套自助门户操作不同地域的云平台的资源；支持异构云平台纳管，包含但不限于 OpenStack、vCenter 等。 2、支持云资源转交功能，管理员创建的云资源可转交给其他用户使用。 3、提供向导式资源操作界面，简化平台的操作难度。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		4、提供在线帮助功能，提供平台常见操作和问题的知识库。 5、提供资源统计功能，支持按照部门或项目统计云资源的使用情况。 售后及实施服务要求 提供 7×24 小时电话支持及两小时上门服务。提供厂商针对本项目的原厂授权函与原厂售后服务承诺函。 对于因产品本身质量原因导致的重大故障，需保证一小时内恢复业务 原厂 3 年维保服务，提供原厂工程师现场实施方案规划、部署、调优、巡检和培训服务。保修期内提供文档知识库、邮件支持、季度巡检以及升级软件版本服务。			
	云运维平台	知识产权要求 1、 与云资源管理平台软件为同一品牌，能够实现与云资源管理软件的无缝对接。厂商须掌握软件自主知识产权，并提供软件著作权证书。 售后及实施服务要求 提供 7×24 小时电话支持及两小时上门服务。提供厂商针对本项目的原厂授权函与原厂售后服务承诺函。 对于因产品本身质量原因导致的重大故障，需保证一小时内恢复业务 原厂 3 年维保服务，提供原厂工程师现场实施方案规划、部署、调优、巡检和培训服务。保修期内提供文档知识库、邮件支持、季度巡检以及升级软件版本服务。	套	1	
2	备份软件	授权许可 备份软件本次配置 16TB 前端容量授权，包含所有的备份功能 为便于存储业务管理及兼容性，要求备份软件与数据存储、备份存储同一品牌 功能 支持主流 UNIX、Linux 和 Windows 与 OpenVMS、Mac OS X Server、Novell、Sun Solaris (SPARC)、Sun Solaris (x86 and x64)、HP-UX (Itanium & PA-RISC)、AIX、SCO OpenServer、RHEL、SLES、CentOS、Debian、Ubuntu、Scientific Linux 支持 SAP HANA、SAP R3、SAP MAXDB、MYSQL、PostgreSQL、Oracle、Sybase、DB2、SQL Server、Informix、Exchange、Domino 等数据库；对以上数据库的集成备份，无需借助第三方工具或定制脚本。 无限制标准客户端与企业客户端的许可，并提供客户端推送安装功能，降低认为误操作或者实施成本，提供功能截图证明并加盖原厂项目授权章	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		提供系统灾难恢复能力，可以在发生灾难后将整个系统（包括操作系统、驱动程序、应用系统）快速恢复到最近备份时间点配置 备份软件支持安装在主流的操作系统平台上，主要有：UNIX、WINDOWS、LINUX 平台 要求提供中文管理界面，提供方便灵活的全图形化工具来完成备份、恢复、定制、监控等操作，无需编写任何脚本即可完成数据库的备份和恢复操作 对 Oracle 数据库进行备份和恢复时提供全图形化操作,尤其针对 oracle 数据库恢复时，无需手工编写 RMAN 脚本或者在客户端中执行 RMAN 恢复命令。统一通过恢复的 GUI 界面，完成恢复，并支持开启 oracle 数据库，支持 Oracle CDB 与 PDB 模式备份，需提供产品截图并加盖原厂项目授权章 备份文件采用统一专有格式，记录了备份信息的标签和日志信息，保证备份内容的安全性， 支持灵活备份策略的定制，支持备份策略的暂停功能 软件提供备份重复数据删除功能，缩短备份时间，备份软提供源端、服务器端或目标端等多种方式重复数据删除功能 备份软件可以结合虚拟带库实现数据源端重复数据删除，备份软件在源端进行重复数据删除以后，直接通过低带库数据传输给虚拟带库，虚拟带库无需再进行重复数据删除，支持虚拟带库的全局重删技术，并支持虚拟带库作为磁盘介质备份 支持多个备份域环境的统一管理，简化备份操作，实现统一监控与备份管理 配置客户端推送安装功能，同时添加卸载客户端/管理服务器，任何系统都不需要重启，降低认为误操作或者实施成本			
3	网管系统	运行环境 系统必须采用 B/S 架构，管理员只需浏览器即可连接到系统进行各种操作。 产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 产品要求至少能够部署在 Windows 和 Linux 操作系统上，支持 64 位操作系统。 监控性能要求 管理中心的并发监控任务个数可以达到 1000 个 使用界面 系统必须采用基于浏览器的用户界面，至少支持 IE 与 Firefox。为了适应不同用途。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		部署方式 支持单级部署和级联部署，支持分布式部署。 工作台 工作台为用户提供了一个从用户自身业务需要出发使用本系统的快速入口。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为不同角色的用户建立不同维度的仪表板； 仪表板中的每个显示区域都能够放大、缩小、拖动； 系统必须内置基本的仪表板； 资产管理 系统具有资产管理的功能，能够将被管理 IT 资产进行分组、分域的统一维护。 系统支持以资产树的形式显示不同资产区域之间的关系； 系统支持以列表的形式显示某个管理区域中的所有资产清单。 集中设备运行监控 系统能够对各种不同厂商的安全设备、网络设备、主机的性能与可用性进行集中化实时监控 网络设备监控 支持所有支持 SNMP 协议的主流网络设备，包括但不限于路由器、交换机、负载均衡、光纤交换机等； 能够监控网络设备基本属性，以及性能与可用性指标，包括：设备名称、IP 信息、描述、节点状态、运行时间、接口信息、路由信息、网络状态信息、网络性能信息 安全设备监控 支持所有支持 SNMP 协议的主流安全设备； 能够监控安全设备基本属性，以及性能与可用性指标，包括：设备名称、IP 信息、描述、节点状态、运行时间、接口信息、网络状态信息、网络性能信息 主机监控 支持主流版本的 Windows、Linux、AIX、Solaris、HP-UX 等主机和服务器； 能够监控主机基本属性，以及性能与可用性指标，包括：名称、IP、描述、节点状态、运行时间、网络接口信息、CPU 利用率、内存利用率、磁盘利用率、磁盘 IO、文件系统、安装软件、安装服务、运行进程、 网络连接； 报表管理 系统内置了资产、事件、监控、风险等报表报告； 提供内置报表模板；			

序号	名　称	技术参数要求	单位	数量	备注
		支持按照天、月度、季度、年度等时间周期生成报表，并支持邮件自动投递； 支持在报表中以柱状图、曲线图、饼状图方式统计安全报警情况 支持报表报告的导出，导出的格式支持 EXCEL、PDF、DOC、XML、HTML、RTF 等，支持 Office 2007 格式；			
（五）	安全资源				
1	互联边界防火墙	规格参数 机架规格 2U；冗余双电源；配置不少于 5 个千兆电接口，4 个千兆光口；不少于 2 个 USB 接口，1 个 RJ45 串口；最大并发连接数≥400 万，最大吞吐量≥40G，每秒新建连接数≥26 万；支持不少于 2 个扩展插槽；支持防病毒和入侵防御功能，配置不少于三年防病毒特征库和入侵防御特征库升级服务；不少于 3 年设备原厂保修服务。 IPv6 支持 IPv6 地址、地址组配置。 支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。 支持 IPv6 静态路由。 支持 IPv6/IPv4 NAT 地址转化 网络适应性 支持透明、路由、混合、旁路等部署模式； 支持静态路由、动态路由（RIP、OSPF、BGP4） 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT 高可用性 支持主-主和主-备模式 支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断 支持双路 HA 物理心跳线，确保 HA 运行稳定可靠 网络访问控制 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 支持基于策略的流量统计和会话统计 入侵防护 支持并开通网络入侵检测及防御功能 防病毒 支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定 防病毒功能开启后，整机处理性能衰减不超过 30% 系统管理 支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能			
2	IPS	规格参数 机架规格 2U；双电源；不少于 2 个扩展槽位；不少于 6 个千兆电口，4 个千兆光口；支持硬件 BYPASS，不少于 1 个 RJ-45 Console 口，2 个 USB 口；最大并发连接数≥400 万，最大吞吐量≥20G；每秒新建连接数≥15 万；特征库＞6000+；不少于 3 年设备原厂保修服务，不少于 3 年 IPS 特征库升级服务。 入侵防护 支持对网络扫描行为的检测和过滤，可实现基于端口的扫描防护和基于主机的扫描防护。 必须支持 IP/MAC 地址绑定的方式防止 ARP 欺骗，可采用手动建立或自动探测的方式生成 IP/MAC 对。 至少支持丢弃封包、切断会话、攻击重定向、记录日志、邮件报警、声音报警 7 种响应方式。 网络适应性 支持透明、路由、混合、旁路等部署模式；	台	2	
3	VPN 设备	规格参数 机架规格 2U；双电源；不少于 1 个 RJ45 口，2 个 USB 接口；不少于 6 个 10/100/1000Base-TX 接口,4 个 SFP 插槽；最大并发连接数≥220 万，每秒新建连接数≥6 万，最大吞吐量≥5G；IPSEC 隧道数≥8000，加解密吞吐率≥400Mbps，SSL 吞吐率≥400Mbps，SSL 并发连接数≥5.4W，SSL 每秒新建连接数≥650，SSL 并发用户数≥3000；客户端许可≥600 个，不少于 3 年设备原厂保修服务； IPSEC VPN 功能 支持标准 IPSEC 协议，能够与 CISCO、JUNIPER 等知名厂商的 VPN 设备互联互通 IPSEC VPN 支持网关、单臂部署模式，IPSec VPN 支持透明、路由、混合等网络环节的接入 支持 AES128/256、DES、3DES、GCM、CCM 等多种加密算法。 支持 AH 和 ESP 封装模式以及 MD5、SHA1、SHA2_256/384/512 等通用摘要算法 支持 DH1、DH2、DH5、DH14 等 DH 组；RSA1024 等非对称加密算法	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		可扩展支持国密版加密算法 SM1/SM4/SM3/SM4 支持多出口 VPN，且支持双向 NAT 穿越（本端 SNAT,对端 DNAT），可配置本地和对端 ID SSL VPN 支持虚拟门户，可以为多个不同区域用户个性化定制多个登录界面，实现不同区域用户可通过不同门户登陆系统 单点登录支持证书主题属性选择，支持根据读取属性分配用户权限 支持三层隧道模式，可使用 SSL VPN 实现三层隧道的加密传输 用户认证 支持本地认证、口令认证、动态令牌、短信认证等多种认证方式，灵活的多认证因子的同时使用 支持基于角色的资源授权，包含 BS、CS、NC 以及资源映射等资源。 支持基于角色及用户组的策略控制，包括归属于该角色的用户认证策略、准入策略、客户端策略等 客户端 支持浏览器自动启动客户端，包含 IE、Firefox、Chrome 等 VPN 客户端支持 MICROSOFT WINDOWS XP、WINDOWS SERVER 2008、WIN7、WIN8、WIN10、CentOS、Redhat 等操作系统 支持 IOS/Android 手机自带 VPN 功能接入 VPN 设备，无需安装任何客户 访问控制 基于源/目的 IP 地址、MAC 地址、域名、端口或协议、服务、网口、时间、用户的访问控制 实现 IP/MAC 地址绑定，且支持 IP/MAC 地址对的自动探测和唯一性检查			
4	链路边界防火墙	规格参数 机架规格 2U；冗余双电源；配置不少于 5 个千兆电接口，4 个千兆光口；不少于 2 个 USB 接口，1 个 RJ45 串口；最大并发连接数≥400 万，最大吞吐量≥40G，每秒新建连接数≥26 万；支持不少于 2 个扩展插槽；支持防病毒和入侵防御功能，配置不少于三年防病毒特征库和入侵防御特征库升级服务；不少于 3 年设备原厂保修服务。 IPv6 支持 IPv6 地址、地址组配置。 支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		支持 IPv6 静态路由。 支持 IPv6/IPv4 NAT 地址转化 网络适应性 支持透明、路由、混合、旁路等部署模式； 支持静态路由、动态路由（RIP、OSPF、BGP4） 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT 高可用性 支持主-主和主-备模式 支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断 支持双路 HA 物理心跳线，确保 HA 运行稳定可靠 网络访问控制 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 支持基于策略的流量统计和会话统计 入侵防护 支持并开通网络入侵检测及防御功能 防病毒 支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能； 支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定 防病毒功能开启后，整机处理性能衰减不超过 30% 系统管理 支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能			
5	视频边界防火墙	规格参数 机架规格 2U；冗余双电源；配置不少于 5 个千兆电接口，4 个千兆光口；不少于 2 个 USB 接口，1 个 RJ45 串口；最大并发连接数≥400 万，最大吞吐量≥40G，每秒新建连接数≥26 万；支持不少于 2 个扩展插槽；支持防病毒和入侵防御功能，配置不少于三年防病毒特征库和入侵防御特征库升级服务；不少于 3 年设备原厂保修服务。 IPv6 支持 IPv6 地址、地址组配置。	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。 支持 IPv6 静态路由。 支持 IPv6/IPv4 NAT 地址转化 网络适应性 支持透明、路由、混合、旁路等部署模式； 支持静态路由、动态路由（RIP、OSPF、BGP4） 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT 高可用性 支持主-主和主-备模式 支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断 支持双路 HA 物理心跳线，确保 HA 运行稳定可靠 网络访问控制 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 支持基于策略的流量统计和会话统计 入侵防护 支持并开通网络入侵检测及防御功能 防病毒 支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能； 支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定 防病毒功能开启后，整机处理性能衰减不超过 30% 系统管理 支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能			
6	对外边界防火墙	规格参数 机架规格 2U；冗余双电源；配置不少于 5 个千兆电接口，4 个千兆光口；不少于 2 个 USB 接口，1 个 RJ45 串口；最大并发连接数≥400 万，最大吞吐量≥40G，每秒新建连接数≥26 万；支持不少于 2 个扩展插槽；支持防病毒和入侵防御功能，配置不少于三年防病毒特征库和入侵防御特征库升级服	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		务；不少于 3 年设备原厂保修服务。 IPv6 支持 IPv6 地址、地址组配置。 支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。 支持 IPv6 静态路由。 支持 IPv6/IPv4 NAT 地址转化 网络适应性 支持透明、路由、混合、旁路等部署模式； 支持静态路由、动态路由（RIP、OSPF、BGP4） 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT 高可用性 支持主-主和主-备模式 支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断 支持双路 HA 物理心跳线，确保 HA 运行稳定可靠 网络访问控制 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 支持基于策略的流量统计和会话统计 入侵防护 支持并开通网络入侵检测及防御功能 防病毒 支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能； 支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定 防病毒功能开启后，整机处理性能衰减不超过 30% 系统管理 支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能			
7	对内边界	规格参数 机架规格 2U；冗余双电源；配置不少于 5 个千兆电接口，4 个千兆光口；不少于 2 个 USB 接	台	2	

序号	名　称	技术参数要求	单位	数量	备注
	防火墙	口，1 个 RJ45 串口；最大并发连接数≥400 万，最大吞吐量≥40G，每秒新建连接数≥26 万；支持不少于 2 个扩展插槽；支持防病毒和入侵防御功能，配置不少于三年防病毒特征库和入侵防御特征库升级服务；不少于 3 年设备原厂保修服务。 IPv6 支持 IPv6 地址、地址组配置。 支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。 支持 IPv6 静态路由。 支持 IPv6/IPv4 NAT 地址转化 网络适应性 支持透明、路由、混合、旁路等部署模式； 支持静态路由、动态路由（RIP、OSPF、BGP4） 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT 高可用性 支持主-主和主-备模式 支持 HA 设备之间的会话自动同步，包括主主模式和主备模式，确保 HA 切换时业务不发生任何中断 支持双路 HA 物理心跳线，确保 HA 运行稳定可靠 网络访问控制 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 支持基于策略的流量统计和会话统计 入侵防护 支持并开通网络入侵检测及防御功能 防病毒 支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能； 支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定 防病毒功能开启后，整机处理性能衰减不超过 30% 系统管理 支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统			

序号	名　称	技术参数要求	单位	数量	备注
		一升级等功能			
8	数据库审计	规格参数 机架规格 2U；冗余电源；不少于 6 个 10/100/1000M Base-TX 接口；盘容量≥4T，入库速度≥25000 条/秒，日处理事件数≥15000 万条；不少于 3 年设备原厂保修服务及软件升级。 审计协议 支持对 Oracle、SQL-Server、DB2、Informix、Sybase、 MySQL、PostgreSQL、Teradata、Cache、MongoDB 数据库进行审计 支持人大金仓 KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) 支持 FTP、Rlogin、Radius、NFS、X11 等协议审计 审计能力与效果 审计策略支持时间、源 IP、目的 IP、协议、端口、登陆账号、命令作为响应条件 支持对数据库绑定变量方式访问的审计 支持访问数据库的源主机名、源主机用户的审计 支持 SQL 操作响应时间的审计 支持审计网络邻居的用户名、读写操作、文件名等 支持审计 NFS 协议的用户名、文件名等 支持审计 Radius 协议的认证用户 MAC、认证用户名、认证 IP、NAS 服务器 IP 支持 IP-MAC 绑定变化情况的审计 支持对针对数据库的 XSS、SQL 注入攻击行为进行审计 事件查询统计与报表 支持按时间、级别、源\目的 IP、协议名、源\目的 MAC、源\目的端口为条件进行查询 支持按数据库名、数据库表名、字段值、数据库登陆账号、数据库操作命令、数据库返回码、SQL 响应时间、数据库返回行数作为查询和统计条件 提供缺省的报表模板库，包括 SOX 报表、PCI 报表等模板，供用户选择使用。 系统应内置统计分析模板，统计模板包括且不限于：趋势分析、统计分析、性能分析等，且支持自定义模板，自定义条件包括源 IP、目的 IP、资源账号、客户端名称、协议等 10 几种。	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		系统支持根据自定义关键字自动生成报表 支持按每天、每周、每月、时刻生成报表 支持生成 Word、PDF、xls、HTML 格式的报表导出			
9	负载均衡	规格参数 机架规格 1U；单电源；不少于 6 个千兆电口，4 个千兆光口，1 个 RJ-45 Console 口，2 个 USB 口，硬盘≥64G SSD，内存≥8G；并发连接数≥800W，每秒新建连接数≥30W，最大有效吞吐≥10G；不少于 3 年设备原厂保修服务。 部署模式 支持路由、旁路部署，以及三角传输 高可用性 支持标准 VRRP 协议 N+1 集群部署：可以实现两台以上设备集群部署，多台设备同时负载一台设备在线备份，集群设备可以是不同的软件版本和型号 四层服务器负载均衡 支持轮询、加权轮询、最小连接、加权最小连接、静态就近性、动态就近性、全局可用、备选 IP、最小流量、最小带宽。 对于源，目的 IP 相同的 UDP 访问，可以对每个报文进行分类转发，保证流量负载的均衡性。 可以对 Radius 等接入认证服务器做基于用户的负载均衡，并且保证每个用户的请求分发到相同的服务器. 服务器过载保护：支持服务器每秒新建连接和会话数限制，保证分担任务不超过其负载能力。 支持通过 Vcenter 自动获取虚拟机状态，并将流量根据配置的负载均衡算法自动分配到各虚拟机。支持虚拟机管理，可监控虚拟机 cpu 占用率，内存占用率，健康状况，连接数等的状态；并根据以上条件对虚拟机进行关闭，挂起，重启，开启等操作。 7 层服务器负载均衡 通过应用层代理，可解析客户端请求内容， 并根据客户端请求头域做内容分发，将访问不同内容的请求代理到相应服务器上；并将响应数据代理到对应客户端。例如对图片类、文字类的请求，分别转发到对应的图片、文字服务器，支持基于 Cookie、User-Agent、URL、HTTP 头的分担模式。	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		服务器敏感信息保护：HTTP 头擦除、重定向信息改写、COOKIE 加密 设备接收到的 HTTP 流量时，可以按指定的规则对其内容进行管理，完成对出入的 HTTP 流量的检查、过滤、修改。主要包括：合规性检查、报文内容修改、重定向等功能。 支持 Http 协议重写，可以把 HTTP 请求自动重写为 HTTPS 协议，实现 HTTP 到 HTTPS 的无缝切换 全局负载 支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括 A ，NS，CNMAE，TXT，MX，PTR 记录。 支持 DNS 授权区域，可将 DNS 名称空间划分为区域来进行管理。可转发 DNS 请求，支持 forward-only forward-first 两种 DNS 转发模式。 支持地域优先、静态就近性、动态就近性 、基于权重、基于 session、基于服务器数量。 支持配置信息同步、状态信息同步。 基于 DNS 方式，在不同地域数据中心之间实现流量牵引。 界面及安全管理 支持全中文的管理界面和 HTTPS 方式登录 支持角色管理、多级授权管理。			
10	堡垒机	规格参数 机架规格 2U；双电源；不少于 6 个 10/100/1000M Base-TX 接口，不少于 1 个接口扩展槽位；存储容量≥3TB，要求支持 raid5；内存≥16G；不少于 1500 路字符会话或 400 路图形会话并发；被管理资源≥1000 个，支持无限个资产管理的扩展能力；不少于 3 年设备原厂保修服务及软件升级； 产品架构 专用安全操作系统，软硬件一体化 部署方式 物理旁路，逻辑串联模式，不影响现有网络结构 单机部署、双机热备部署 支持 NAT 地址映射部署，通过映射后的 IP 地址访问堡垒机进行管理和运维操作，支持从多个映射地址访问，适用于内外网隔离的复杂网络环境 管理分权 系统级账号三权分立，系统级账号包括：系统账号管理员，系统审计员，系统管理员 业务管理组：分属不同业务管理组的业务管理员只能管理所在业务管理组内的用户、资源、策略和审计管理，适用于不同的管理部门有独立的管理员，运维人员，资源和审计管理要求的场景	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		用户和资源管理范围：可设置业务管理员可管理的用户组和资源组的范围，适用于部门内管理员管理用户和资源权限的进一步划分 用户管理 支持用户和用户组的管理，包括添加、修改、删除、启用、停用、移动和移除组成员功能 支持用户账号的批量导入导出功能 支持设置用户属性为：不能修改密码、密码永不过期、下次登录必须更改密码 用户密码策略包括：最小密码长度、密码复杂度、密码周期、历史比对和登录锁定 支持用户账号有效期配置 资源管理 支持资源和资源组管理功能，包括添加、修改、删除、启用、停用、移动和移除组成功功能 支持资源（包括服务和资源账号）批量导入导出功能 支持资源自动发现和添加，便于快速添加资源 资源密码管理 支持设定周期性改密计划，批量修改资源密码 支持手动改密，修改指定资源的账号密码 自动改密密码策略支持随机生产不同密码 、随机生成相同密码 、手工指定相同密码，随机密码支持自定义密码强度 实时监控 实时监控当前连接发生的所有会话信息，发现高危操作可实时切断会话 会话回放 WEB 在线视频回放方式重现维护人员对服务器的所有操作过程 离线回放重现维护人员对服务器的所有操作过程（回放文件下载到本地播放） 身份认证 支持本地账号+密码认证；USB-KEY 认证；动态口令认证；短信认证；数字证书认证和其他外部认证等。 双因素认证：支持对不同用户设置不同认证方式组合的双因素认证			
11	APN 防火墙	规格参数 机架规格 2U；冗余电源；不少于 6 个 10/100/1000M Base-TX 接口，4 个千兆光口；不少于 2 个 USB 接口，1 个 RJ45 串口；最大并发连接数≥320 万，最大吞吐量≥10G，每秒新建连接数≥8 万；不少于 3 年防病毒库升级授权，3 年 IPS 特征库升级授权；不少于 3 年设备原厂保修服务；	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		IPv6 支持 IPv6 地址、地址组配置。 支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT 网络适应性 支持静态路由，动态路由（OSPF、RIP、BGP） IPSEC VPN IPSec VPN 支持网关、单臂部署模式 IPSec VPN 支持透明、路由、混合模式等工作模式 支持标准 IPSec、GRE、PPTP 、L2TP、DMVPN 等形态 VPN 。 入侵防护 支持对网络扫描行为的检测和过滤			
12	漏洞扫描	规格参数 机架规格 2U；冗余电源；硬盘≥1T，不少于 1 个 RJ45 串口，2 个 USB 接口，不少于 6 个千兆电口，不少于 1 个接口扩展槽位；单任务可扫描≥256 个 IP 地址，并发扫描≥20IP，主机漏洞知识库≥4000+，不少于 3 年设备原厂保修服务；不少于 3 年漏洞库升级服务； 扫描能力 漏洞扫描方法应不少于 30000 种 漏洞库与 CVE、CNCVE、CNNVD 和 BUGTRAQ 等国际、国内标准兼容 支持在 IPv6 环境中部署和执行扫描任务。 支持扫描 IPv6 环境中的设备、系统 支持对各种网络主机、操作系统、网络设备（如交换机、路由器、防火墙等）、常用软件以及应用系统的识别和漏洞扫描。 支持对扫描对象的脆弱性进行全面检查，识别内容应包括操作系统和应用系统安全补丁的缺失、弱口令、常见木马后门、不安全的服务配置等。 支持多种协议口令猜测，包括 Telnet、Pop3、SSH、Ftp、RDP、SQL Server、DB2、MySQL、Oracle 等；允许外挂用户提供的字典档。 支持自动发现和识别目标主机的操作系统类型，并根据其系统类型选择对应的扫描方法。	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		支持实时显示扫描进度以及阶段性扫描结果，包括主机名、开放端口、操作系统、服务、用户、BANNER信息、漏洞信息等。 支持对意外中断（网络中断、设备断电）的扫描任务恢复后继续进行扫描； 支持扫描任务优先级设置； 策略管理 支持至少 17 种以上默认扫描策略。 支持灵活的扫描策略自定义功能，提供策略编辑向导和详细漏洞信息，支持以系统类型、漏洞类型、危险级别、CVE 等不同视图显示漏洞，支持策略的导入、导出、修改以及合并 支持对端口范围、CGI 扫描、后门、用户名密码字典、数据库扫描、SNMP 扫描、主机存活探测等多种通用扫描参数进行详细自定义。 资产管理 支持对部门和资产的添加、删除、编辑等操作，以及对资产的属性自定义功能； 支持以 txt、csv、dat 等格式进行资产列表的导入。 资产自动发现，支持利用历史扫描过程中所发现的在线主机信息，来添加部门的资产； 支持对已有的资产和部门直接扫描； 支持显示资产和部门的历史扫描结果，支持显示资产和部门的风险评估值； 报表功能 报告应包含漏洞详述和修补方案，对于常见补丁类漏洞能够提供相关的补丁下载链接。 支持生成同一任务的不同时间段扫描结果的对比报告。 支持用户自定义扫描报告模板。 支持导出 html、word、excel、PDF 等多种常见格式报表。 支持自动报表功能，扫描完成后可以自动生成报表，并以邮件形式自动发送到指定接收人和邮件组。 对于周期任务，支持自动把与最近一次扫描结果的对比报告发送给管理员，以及时了解新增威胁。			
13	防毒墙	规格参数 机架规格 2U；冗余电源；不少于 6 个 10/100/1000M Base-TX 接口，4 个千兆光口；不少于 2 个 USB 接口，1 个 RJ45 串口；最大并发连接数≥360 万，最大吞吐量≥20G，每秒新建连接数≥15 万；不少于 2 个扩展插槽；不少于 3 年 AV 特征库升级及设备原厂保修服务；	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		IPv6 支持 IPv6 地址、地址组配置。 支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、扩展头属性等条件进行安全访问规则的设置。 支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT 支持 IPv6 静态路由。 网络适应性 支持静态路由，动态路由（OSPF、RIP、BGP） 入侵防护 支持对网络扫描行为的检测和过滤 防病毒 支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能； 支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定			
14	日志审计系统	产品基本功能 网络安全日志审计系统平包括资产管理、安全事件管理、基础分析、首页、主机操作系统、网络设备、安全设备日志收集，查询，告警，审计，报表等功能、标准的响应管理模块、权限管理、系统自身管理、本地事件采集器，配置不少于 200 个审计对象授权 提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表； 采集方式 无需另外安装软件组件，审计中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFPT、NetBIOS、OPSEC 等多种方式完成日志收集功能； 资产管理 系统具有资产管理的功能，能够将被审计资产进行分组、分域的统一维护。 系统支持以资产树的形式显示不同资产区域之间的关系； 系统支持以列表的形式显示某个管理区域中的所有资产清单； 系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点 能够根据收到的事件的设备地址自动识别新的资产，并支持自动添加到资产清单中去； 在资产管理界面可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表。	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		日志范式化 系统必须具备日志范式化功能，实现对异构日志格式的统一化； 范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等； 日志分析 系统允许管理员实时的，以监视场景的形式查看不同类型的日志信息； 用户可自定义监视场景，每个监视场景都要以监视策略的形式进行存储，并形成一个监视树； 实时显示日志内容包括：接收时间、事件类型、事件名称、报警级别、来源 IP、目的 IP、设备类型、设备来源 IP 等。 可查看日志详细信息和原始信息。 可查看日志的参考说明。 日志告警 告警动作支持告警重定义、弹出提示框、发出警示音、发送邮件、发送 SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送 Syslog 等方式； 日志传输和存储转发 日志可加密压缩传输，保证数据的完整性和机密性； 日志可加密存储。支持大数据量存储；			
（六）	专用设备				
1	互联网访问控制系统（前置）	功能要求：与互联网访问控制系统（前置）配套使用,提供请求和响应报文接收、解析、转换、发送等功能；设置安全策略对共享服务进行访问控制。 稳定性运行时间(MTBF)：>50,000 小时； 性能要求：并发用户数量：≥5000 个；每秒钟传输数据量：≥4Gbps；最大传输延时：<2s； 设备管理要求：支持采用基于 HTTPS 安全协议的管理方式； 协议支持：支持 SYSLOG、SNMPX 协议； 操作系统：采用基于 Linux 操作系统内核剪裁、增强、优化的安全操作系统； 网络接口：千兆以太网口≥6，万兆光口≥2 个。	台	4	

序号	名　称	技术参数要求	单位	数量	备注
		网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。			
2	互联网访问控制系统（后置）	功能要求：与互联网访问控制系统（前置）配套使用,提供请求和响应报文接收、解析、转换、发送等功能；设置安全策略对共享服务进行访问控制。 稳定性运行时间(MTBF)：>50,000 小时； 性能要求：并发用户数量：≥5000 个；每秒钟传输数据量：≥4Gbps；最大传输延时：<2s； 设备管理要求：支持采用基于 HTTPS 安全协议的管理方式； 协议支持：支持 SYSLOG、SNMPX 协议； 操作系统：采用基于 Linux 操作系统内核剪裁、增强、优化的安全操作系统； 网络接口：千兆以太网口≥6，万兆光口≥2 个。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。	台	4	
3	单向光闸	功能要求：采用物理单向传输技术，实现数据或文件的单向数据导入，与导入前置机和导入服务器的文件传输进行双向认证，对用户权限进行统一分配和管理，保证文件数据传输的完整性，导入前置机发送的数据和导入服务器接受的文件保持一致，对传输的数据业务进行日志审计。 管理功能：采用基于 HTTPS 安全协议的管理方式； 协议支持：支持 SYSLOG 协议；支持 SNMPX 协议； 吞吐量 ≥4Gbps； 内端机：系统采用工业级服务器体系架构，背板交换带宽:>10Gbps。操作系统：采用基于 Linux 操作系统内核剪裁、增强、优化的安全操作系统。千兆以太网口≥6 个，万兆网口≥2 个。	台	4	

序号	名　称	技术参数要求	单位	数量	备注
		外端机：系统采用工业级服务器体系架构，背板交换带宽:>10Gbps。操作系统：采用基于 Linux 操作系统内核剪裁、增强、优化的安全操作系统。千兆以太网口≥6 个，万兆网口≥2 个。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。			
4	视频安全接入系统（前置）	功能要求：能支持视频组播；支持标准 SIP 协议,对于视频厂商实现了标准 SIP 协议的直接转发 支持标准 TCP/UDP 数据传输。对视频厂商实现了 TCP/UDP 代理协议转发。支持标准视频点播协议（H.264、H.263、RTSP），并可对协议进行分析和审核。 硬件规格：网络接口≥6 个 10M/100M/1000M 自适应以太网接口； 性能参数：最大并发连接数≥ 2000；最大网络流量≥800Mbps；支持≥400 路 D1 图象（2Mbps）或 100 路高清 8Mbps； 管理能力：采用基于 HTTPS 安全协议的管理方式；支持 SYSLOG、SNMPX 协议。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。	台	2	
5	视频安全接入系统（后置）	功能要求：能支持视频组播；支持标准 SIP 协议,对于视频厂商实现了标准 SIP 协议的直接转发 支持标准 TCP/UDP 数据传输。对视频厂商实现了 TCP/UDP 代理协议转发。支持标准视频点播协议（H.264、H.263、RTSP），并可对协议进行分析和审核。 硬件规格：网络接口≥6 个 10M/100M/1000M 自适应以太网接口； 性能参数：最大并发连接数≥ 2000；最大网络流量≥800Mbps；支持≥400 路 D1 图象（2Mbps）或 100 路高清 8Mbps； 管理能力：采用基于 HTTPS 安全协议的管理方式；支持 SYSLOG、SNMPX 协议。 网络能力 支持 IPv6	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。			
6	视频网闸	基本要求：内、外网分别具有独立的管理接口，不是通过网络接口管理;内、外网分别具有独立的 HA 口，实现双机热备及负载均衡;内外网主机系统与专用隔离部件之间采用高性 PCI-E 总线连接，消除性能瓶颈;提供完善的日志审计;提供设备运行状态检测、系统资源监控。 硬件规格：2U 机箱，内外端机各≥6 个 10/100/1000Base-T(RJ-45)接口，2 个万兆光口；系统吞吐量≥900Mbps；延时≤20us； 协议支持：支持 HTTP/HTTPS/FTP/SMTP/POP3 等应用协议;支持 H323/H323_GK 等多媒体协议；支持 SNMP/DNS 等网络协议； 视频编码格式支持：支持 M-JEPG，MPEG4、H.264、H.323 等编码格式； 视频分辨率：支持 D4、D1、VGA、2/3D1、1/1.8D1、SIF、3/4D1、CIF、QCIF； 硬件架构：系统内部采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块；内外端机为网络协议终点，彻底阻断各种网络协议， 保证信任网络和非信任网络之间链路层的断开，彻底阻断 TCP/IP 协议以及其他网络协议。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。	台	2	
7	网络接入控制系统	基本功能：支持自动发现网络上的所有接入设备，并对设备进行定位；支持自动检查接入终端的安全状态，支持自定义检查规则，检查内容包括：用户帐号、操作系统安全设置、防病毒软件状态、接入位置、终端硬件信息等；支持自动隔离不安全的终端，并为其提供自助修复环境；支持访问时长、限定终端硬件属性的访问控制列表；支持多样化准入方式，从基本的接入身份标识到接入后的合规检查、修复向导以及安全审计等；支持直接与网络设备联动，自动下发 VLAN 和 ACL。 硬件规格：标准 2U 机箱，10/100/1000MBase-TX 网口数≥6 个；SPF+模块与插槽≥2 个；CPU：4 核，支	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		持超线程 4 核；电源标配：冗余电源； 性能要求：最大并发用户数≥3 万；终端接入速度≥5000 个/s；吞吐量吞吐率≥8Gbps。 网络能力 支持 IPv6 用户接入控制：可实现基于数字证书、终端身份、安全状态的用户接入控制，提供相关证明文件，并加盖原厂商公章。			
8	身份鉴别认证系统	基本信息管理：需提供统一的机构和用户管理，支持机构、用户同步功能。 对接能力：对接包括但不限于代理网关、应用系统、总线系统，为民警和协辅警提供统一的认证和授权服务。 统一认证授权：认证的方式需要支持依托于 PKI 的证书方式认证，针对无证书的用户，也需要支持口令认证和对接生物认证。授权的方式需做到灵活多样，可以支持用户、组织机构，用户组、用户属性（警种、职务等）授权。 性能要求：支撑用户数≥8 万；认证请求并发支持要求≥1000 次/秒。	台	1	
9	代理网关	功能要求：实现统一的服务资源标准接口封装及授权调用。为各类应用所需调用的服务资源提供统一标准、可管可控的接口服务，减少数据资源的重复使用、不可控的混乱使用情况。此子系统分别部署在移动互联网服务子平台、联网服务子平台和公安信息网服务子平台，通过低层封装上一层的方式，分别为Ⅰ、Ⅱ、Ⅲ类应用提供服务。 基本信息管理：需提供统一的机构和用户管理，支持机构、用户同步功能。 性能要求：支撑用户数≥10 万；吞吐量 ≥800Mbps；认证请求并发支持要求≥1000 次/秒。	台	2	
10	网络探针	主要功能：采集公安内网所有设备的运行状态，包括 CPU、内存、网络等使用情况以及由操作系统产生的各类异常告警信息等；采集公安内网主要安全设备和业务系统的业务运行日志、管理员管理操作日志以及系统告警信息等；获取集中监管与审计系统、统一运维系统的管理参数，对公安内网网络设备的网络信息进行联动管理；支持与集中监管与审计系统的交互，获取对终端用户的管控策略；支持对采集的数据按照后台系统提供的规则进行数据清洗、抽取、分析，实现对用户流量、应用流量、应用访问频次	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		的统计，并在此基础上对安全事件进行告警记录；支持与公安内网的统一运维系统对接，实现实时掌握设备状态，进行跨网版本升级、配置更新等统一维护操作。 协议支持：将通过 SYSLOG、v2/SNMP v3、Telnet、ICMP 等方式获取到的信息传输给内网集中监控管理系统；支持 SYSLOG、v2/SNMP v3、Telnet、ICMP 协议； 管理功能：使用基于 HTTPS 方式的管理设备； 稳定性运行时间(MTBF)：＞50000 小时； 网络接口：≥6 个千兆网络接口； 性能要求：吞吐量≥800Mbps；支持≥200 个采集单元。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。			
11	数据探针	功能要求：采集所在区域业务数据，按照过滤策略进行敏感数据报警、接收数据副本功能； 数据清理后进行上报集控中心。 协议支持：SYSLOG、v2/SNMP v3、Telnet、ICMP； 管理功能：使用基于 HTTPS 方式的管理设备 稳定性运行时间(MTBF)：＞50000 小时 产品尺寸：标准机架 1U 设备 网络接口：6 个千兆网络接口 性能要求：吞吐量≥800Mbps；支持≥200 个采集单元。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。	台	1	
12	安全管控系统	主要功能： 1) I 类区各要素数据采集。按照《移动警务安全管控接口规范 20180921》标准与移动互联网服务子平台内其他系统及网络设备对接，对接范围包括本区域应用支撑系统、主机服务器、网络设备、安全设备	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		等。 2）Ⅰ类区数据分类处理。将采集的数据信息进行存储、分类预处理、归并和压缩等操作。 3）Ⅰ类区策略接收下发。接收集中管控中心控制策略，并下发到Ⅰ类区管控指令执行系统和网络设备。 4）Ⅰ类区级联数据上报。将Ⅰ类区分类处理后的格式数据上报集中管控中心。 部署要求：支持通用服务器部署； 性能要求：支持与≥200 个设备对接，支持与≥200 个应用系统对接；解析处理能力 ≥800 条每秒； 网络能力，不少于千兆网口×2，支持 IPv6 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。			
13	智能移动终端管理（MDM 系统）	总体管控方案 提供一套完整的多模式警务终端安全管控方案，包含多模式警务终端安全管控平台。要求安全监控组件内置于多模式警务终端，对一台终端上的生活模式和工作模式分开管理，能够实现基本管理、设备管理、网络管理、通话管理、多模式管理、应用管理、安全管理等功能。 按照《全国公安移动警务建设总体技术方案（2016 版）》规定，针对可访问互联网的Ⅰ类系统，移动智能终端生活模式下可以安装移动警务Ⅰ类系统应用，以及个人所需要的软件，提供终端互联网使用便利。 在此类场景中管控平台对终端提供必须的辅助管理功能： 1）移动智能终端丢失后可以提供安全管控策略，对终端进行锁机或全终端数据销毁； 2）与管控平台同步系统时间，同时禁止修改普通系统的系统时间； 3）发生工作 SIM 卡和安全 TF 卡拔出、更换等异动，立即对终端进行锁机或全终端数据销毁； 4）禁止终端在 Ⅰ 类系统中手工配置工作的 APN 参数； 5）禁止终端在 Ⅰ类系统中热点共享工作用的 APN 接入点。 针对Ⅱ类、Ⅲ类安全系统，智能终端运行在工作模式下，将完全运行内部移动警务应用，同时需满足如下管控要求： 基本管理 终端启用	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		1、预注册：由管理员在后台通过单个或批量方式导入用户信息和终端 IMEI、SIM 卡 IMSI 等信息。 2、终端激活：终端插入 SIM 卡，通过扫描注册二维码，并通过后台导入的用户信息、SIM 卡(IMSI)等验证后，进行关联绑定，并且激活。 3、机卡绑定：管控平台根据终端注册时使用的终端号卡与终端进行一对一绑定。当终端上使用的号卡发生变化时，对终端进行异常行为监管，锁定终端，防止终端的违规使用 终端退役 1、终端丢失：终端发生丢失时支持擦除终端数据并解除人员、终端、SIM 卡绑定关系。 2、终端注销：支持注销终端管理，注销后终端解除管理状态，清空管理指令。 3、终端解绑：通过管理员操作系统后台对原先绑定的终端解除绑定，为人员替换或更换终端、号卡时提供业务服务。 设备管理 1、终端端口管理（开启/关闭）：系统后台可以控制终端上相关端口功能的开启和关闭，包括：蓝牙开启/关闭、摄像头开启/关闭、麦克风开启/关闭、网络访问开关（WIFI 开启/关闭、移动数据开启/关闭）、个人热点开启/关闭、GPS 开启/关闭、USB 调试和 USB 大容量存储功能开启/关闭、SD 卡功能开启/关闭，飞行模式功能开启/关闭，截屏功能开启/关闭，录屏功能开启/关闭 2、终端资产管理：显示终端基本信息，包括：终端号码、用户名称、所属部门、终端状态、是否在线、是否 Root、是否外出、是否失联、最后连接时间等信息。 3、端到端管理：管理员可以通过终端对自己管理权限范围内的终端进行管理，包括锁定终端、寻找终端、盘点终端、发送消息等各项功能。 4、远程协助：管理员通过系统后台对终端发起远程协助，终端接受许可后，管理员在管控 PC 上可以远程接管该终端安全工作模式的界面，针对终端使用的问题，提供远程协助，远程帮助终端使用者解决问题。 5、终端文件管理： 终端文件获取：要去系统能够通过后台获取终端存储空间指定目录中的文件。			

序号	名　称	技术参数要求	单位	数量	备注
		终端文件推送：要求系统能够通过后台对终端存储空间的指定目录中推送文件。 6、离线管理：当终端初始化以及在线的情况下接收到管控后台下发的管控指令和策略后，即使终端处于离线状态下，被预先设置的管控指令和管理策略仍然生效：例如执行锁屏、应用黑白名单管控、应用安装限制、热点分享、限制使用蓝牙、限制使用 USB、限制使用 GPS 等管理。 7、时间围栏：可配置时间围栏的管理动作，当终端到达设定的时间自动触发执行时间围栏配置的管理。 #8、禁止修改终端时间：禁止用户手动修改终端的系统时间，并且可以强制终端与后台的时间基准服务器进行时间同步。 9、地理围栏：可配置地理围栏的管理动作（围栏内或者围栏外），当终端在指定的地理位置时自动触发执行地理围栏配置的管理。 10、离线地图定位：使用离线地图方式，实现内网定位。 11、策略执行跟踪：在策略分配后，可在后台查看策略执行情况：查看策略分配任务执行列表（策略名称、执行人、执行时间）；点击单行展示指令总数、未执行数、已执行数、取消数；终端执行列表明细查看、导出。 12、终端管理状态查询：管理员通过系统后台查询所有注册终端的已注册、在线、失联、外出、Root、已注销等管理状态。 13、蓝牙配对白名单：白名单内的蓝牙设备，终端允许连接，白名单外的蓝牙设备，终端禁止连接 14、WiFi 热点白名单：管控服务平台配置终端 WiFi 热点白名单，终端打开热点之后，仅白名单中的设备可以连接该热点，其他设备无法连接。 网络管理 1、强制开启移动数据：为防止终端与服务器中断链接而脱管，系统可以下发指令强制终端开启移动数据。 2、移动数据卡槽管理：办公模式强制使用工作卡移动数据。生活模式优先使用工作卡移动数据，用户可选择使用个人卡移动数据。 3、专用 APN/VPDN 自动配置和接入：APN/VPDN 配置信息通过系统后推送，终端自动配置和切换到接入网			

序号	名　称	技术参数要求	单位	数量	备注
		APN/VPDN，并且保证接入网 APN/VPDN 配置不可修改，且一直处于保活状态。 4、接入网的 APN/VPDN 批量生成：系统后台支持接入网 APN/VPDN 配置的批量生成。 5、VPN 管理：后台可以配置 VPN 菜单禁用/启用（设置-移动网络-VPN），可以禁用/启用对 VPN 的保活；后台配置 VPN 客户端属性，根据属性自动下载和安装 VPN 客户端。 6、VPN 自动接入：支持在接入网 APN/VPDN 切换成功后，可以自动调用拨通 VPN，并且保活 VPN 连接。 7、禁止网络热点共享　禁止通过 USB 网络分享、蓝牙网络分享以及热点分享功能，防止通过共享网络非法接入内部网络。 通话管理 1、通话功能限制：后台可以控制终端的通话功能的使用，当限制通话功能时，终端不能接听与拨打电话。 双模式管理 为保证用户内部应用和数据的安全性，系统要求支持多模式管理，将生活模式和工作模式分别进行管理，对多模式管理的主要功能如下： 1、登陆认证：终端进入工作模式时，要求输入工作模式密码，同时要求支持三个认证一次性拨通：VPDN，安全链路长链接，TF 卡加密认证，只有通过认证才可以访问工作模式。 2、工作模式管理：工作模式中的数据以加密形式存储，只能被指定的工作模式中的应用打开或访问，禁止工作模式外的应用访问安全容器中的数据。 3、工作模式应用管理：系统支持工作模式专有 App 的上传、审批、下发、安装（静默安装和手动安装）、卸载（静默卸载和手动卸载）、更新（静默更新和手动更新）功能。 4、工作模式网络连接：工作模式通过 APN/VPDN 链路接入，默认禁止 WiFi 数据连接。 5、工作模式锁定/解锁：系统支持在设备出现异常的情况下远程锁定工作模式，使工作模式无法被访问，当确定设备正常后解除锁定。 6、工作模式擦除：系统支持对工作模式远程擦除。 7、控制破解设备对应用的访问：如设备被破解禁止使用指定的应用，工作模式自动被擦除； 8、控制应用数据的拷贝、剪切和粘贴：工作模式内外无法以剪切、复制和粘贴的方式传输数据。			

序号	名　称	技术参数要求	单位	数量	备注
		9、超时登陆：工作模式登录后如果长期在线不使用，再次使用时，用户需要重新登录。 10、应用隔离：工作模式中的应用只能在相应的工作模式中的被打开或访问，禁止被普通工作模式应用访问。 11、数据隔离：生活模式与工作模式中的通话记录、通讯录、图片、视频、应用数据以及其他信息不能互相访问。 12、全设备擦除：管控平台支持远程同时擦除生活模式、工作模式以及 TF 卡数据。 #13、多模式端管控指令分区生效：系统可以对多模式分别制定指令策略，并指定下发给终端不同模式，并在该模式下生效，当终端进行模式切换时，自动生效切入模式的管控策略。 应用管理 1、应用白名单：系统后台支持应用白名单库，支持增、删、改、查、导入操作，安全监控组件仅允许白名单中的应用可以下载安装并使用，禁止终端使用白名单外的应用。 2、应用黑名单：系统后台支持应用黑名单库，支持增、删、改、查、导入操作，安全监控组件禁止安装和使用黑名单中的应用。 3、应用安装功能限制：系统后台可以控制终端安装应用功能的使用，当限制安装功能时，终端上所有的软件安装包均无法安装（包括通过互联网下载、存放在 SD 卡上、通过蓝牙/红外传输、与电脑 USB 连接拷贝安装包）。 4、应用防卸载：禁止用户卸载终端上的应用，包括自带应用和手动安装的第三方应用，可以指定保护某一程序不被卸载。 5、应用静默/强制安装接口：为应用商店提供接口可通过服务器管理端对移动终端下发策略实现应用静默/强制安装。 6、禁用/允许系统自带应用商店：禁止/允许使用系统自带应用商店。并且禁止 USB、TF 卡、下载等其他应用安装途径。 7、软件资产管理：可在终端上查看应用的详细信息，包括：软件名称、包名、版本号、软件大小、是否系统应用、是否白名单应用、安装时间、上报时间等。			

序号	名　称	技术参数要求	单位	数量	备注
		安全管理 1、终端锁机：系统后台可以对终端进行远程锁定，锁定后无法正常使用终端的各项功能，包括拨打、接听电话，发送短信等。 2、修改密码：支持对单台、多台终端修改系统锁屏密码。 3、清除密码：支持对单台、多台终端清除系统锁屏密码。 4、离线密码：后台提供一套算法生成动态离线密码，以避免网络无法连接导致终端锁定后无法解锁。 5、设备级水印：要求系统提供设备级水印，根据需求能够给指定应用或者全设备加载水印。 6、终端异常管理： ROOT：当检测到终端被 Root 后，终端将进行锁机、擦除等等管理。 失联：当检测到终端失联后，终端将进行锁机、擦除等等管理，且管理指令无论是在网或者离线状态下都会生效执行。 7、终端擦除/恢复出厂设置：系统后台可以对单台、多台终端擦除终端数据，将终端恢复出厂设置。 人员组织管理 1、组织维护：系统后台支持分级管理，对部门的增、删、改、查、批量导入。 2、人员维护：系统后台支持人员的增、改、查、批量导入，绑定人员和 IMSI 信息。 3、人员管理：基于一体化平台提供的人员架构进行部署，如果人员调动了，自动推送人员当前部门相关应用并删除之前部门不相关应用。 4、分组管理：除了可根据组织机构的方式进行管理外，后台还可为根据管理要求创建不同的人员分组，通过分组进行策略管理。 系统管理 1、权限管理：后台可创建多个管理员，对管理员可管理的组织机构范围进行设定，从而提供不同权限的管理账户。 2、角色管理：系统后台通过不同管理功能的配置将管理员进行角色化区分。 3、管理员管理：系统后台可对管理员进行增、删、改、查、角色分配，并且支持多级管理员管理结构，上级可管理下级，不可管理与查看上级或平级。 4、修改管理员密码：修改管理员系统登录密码。			

序号	名　称	技术参数要求	单位	数量	备注
		系统监控 1、 已注册数：统计当前管理范围内已注册终端数量。 2、 在线数：统计当前管理范围内在线的终端数量。 3、 越狱数：统计当前管理范围内被 Root 的终端数量。 4、 失联数：统计当前管理范围内离线时间超过设置的失联时间的终端数量。 5、 日新增终端量统计图：以折线图形式展示一周内管理范围内每日新注册终端情况。 6、 日指令发送量折线图：以折线图形式展示一周内管理范围内管理员每日发送指令总数情况。 7、 终端失联监控：实时显示管理范围内的失联终端记录。 可视化监控：要求提供监控指挥中心实时展示终端情况和违规情况，以及人员热力分布图。 报表管理 1、 终端报表：支持终端离线、ROOT、失联（包含失联时间配置小时展示）的查询及导出 2、 限制状态报表：终端限制情况查询分析。展示当前终端蓝牙、摄像头、麦克风、WIFI、移动数据的限制情况。 3、 应用报表：汇总终端上应用的安装情况，按照应用的安装量降序展示，可查看应用的详细安装信息，包括应用名称、包名、版本名称、是否系统应用、终端 ID、终端号码、用户名称、所属部门，支持报表导出功能 4、 流量统计报表：统计应用的使用时长和移动数据流量使用 5、 管理员日志报表：记录管理员的操作日志，支持查询和导出报表 6、 安全监控组件客户端自更新统计：查询统计安全监控组件客户端新版本的更新情况 外部接口 1、单点登录：系统需提供第三方应用统一登录接口，供第三方应用登录认证。在用户登录移动门户后，可直接在门户中启动第三方应用，而不需要二次登录。 2、为第三方应用提供保活接口：提供第三方应用的保活机制，防止第三方应用在息屏、低电量模式下被系统杀掉进程和服务。 强壮性要求 1、安全监控组件防卸载：要求支持安全监控组件卸载保护机制，用户在界面上无法卸载安全监控组件客户端，管理员卸载客户端应用程序需要通过输入卸载密码或通过管理中心指令卸载。			

序号	名　称	技术参数要求	单位	数量	备注
		2、安全监控组件系统权限保活：在终端厂商自带的终端管家中取消安全监控组件的权限，这些权限不能被取消；系统清理内存模式下、低电量模式下安全监控组件进程依然保活 3、软恢复出厂管理：禁止从终端设置界面中恢复出厂； 、硬恢复出厂管理：终端被硬键组合开机后恢复出厂依然被管控； 5、防 ROOT：终端被 ROOT 后立即被锁机或者被擦除； 6、防刷机：终端无法被刷机后脱离管控或挪为他用。 管理平台技术性能参数 在安全接入平台环境下运行，对性能有如下要求： （1）要求系统能够承载管理≥5000 台设备，且能够根据实际需要进行线性扩容； （2）终端管理平台服务器支持并发用户数≥500； （3）实时管控命令反馈：≤5 秒； （4）主动检测巡检时间：≤30 分钟。 资质要求 1.投标人需提供由公安部门颁发的多模终端安全管控系统信息安全等级保护三级及以上认证备案证书，提供证书复印件并加盖厂商公章或投标专用章； 2.投标人所投平台需提供由公安部监制的计算机信息系统安全专用产品销售许可证，提供证书复印件并加盖厂商公章或投标专用章； ▲3.投标人所投平台需提供由中国网络安全审查技术与认证中心颁发的 ISCCC IT 产品信息安全认证证书，提供证书复印件并加盖厂商公章或投标专用章； 4、投标人所投平台需通过 ISO27001 信息安全管理体系认证，提供证书复印件并加盖厂商公章或投标专用章； 5、投标人所投平台需通过 ISO9001 质量管理体系认证，提供证书复印件并加盖厂商公章或投标专用章；			
14	短信网关	支撑能力 支持移动、联通、电信“三网合一”短信网关 短信网关协议 CMPP2、CMPP3、CMPPE、SMGP、SGIP 认证能力 每秒≥25 次	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		处理能力 每秒处理条数≥100 条，			
15	网络流量分析系统	整机 2UX86 服务器架构，冗余双电源； 双 Intel E5-2630v4 CPU 或以上,共 20 个物理核以上；内存 64GB、硬盘容量 44TB 以上，配置硬件 2G 缓存 RAID 卡; 配置≥2 个万兆 SFP+光口,≥4 个千兆电接口 最大流量处理能力 20Gbps，最大报文存储性能 10Gbps，最大并发用户数 10 万， 最大并发会话数 400 万，最大新建会话数 20 万/秒 功能 基于 B/S 架构进行管理和流量数据分析，能够分布式部署在各个监控的网络节点，实时分析捕获流量,实时保存捕获到的网络通讯数据包，进行长时间、大容量的数据存储能力 ▲采用软硬件一体化设计，通过 WEBUI 直接进行流量回溯、流量可视化的查看、搜索；要求提供功用截图并加盖原厂项目授权章 支持交换机镜像、路由器镜像、分光器、网络分流器等部署方式，支持以太网、POS 接口流量镜像分析，旁路部署，对网络整体架构无影响 支持离线报文远程解码分析，支持源端回溯系统存储报文通过 WEB 进行协议解码（不需要下载到本地）、时序图展示、HTTP 等内容还原；要求提供功用截图并加盖厂商项目授权章 能够实时捕获并保存网络中的通讯数据包，存储时间可以根据硬盘大小进行调整 能实时分析并长期保存网络中的所有数据流统计数据，包括详细的 IP 会话流、TCP 会话流、UDP 会话流数据，数据精度到秒级，数据流统计数据要求能保存至少 1 个月； 支持基于 1 秒、10 秒、1 分钟、10 分钟几种颗粒度进行回溯展示； 支持在线用户、用户历史流量、用户实时流量、用户中心展示，可以查看用户终端、用户虚拟画像、用户与应用流量的二级钻取；要求提供功用截图并加盖原厂项目授权章 支持应用的实时流量、历史流量、应用质量、未知应用可视化呈现、展示 支持服务器的实时流量、会话统计，支持服务器历史流量会话统计，支持单个服务器下的用户流量、会	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		话统计；要求提供功用截图并加盖原厂项目授权章 支持行为呈现的数量趋势图、各行为类型分布饼图、以及各行为的表格数据，各行为可以二级钻取，查看 TOP10 的排名以及 TOP10 用户访问; 视频监控网络质量进行分析，分析流量、流量突发、网络丢包、网络时延、网络抖动等业务指标，针对摄像头、业务服务器进行质量排名；要求提供功用截图并加盖原厂项目授权章 支持视频监控网络流量异常（流量中断、突发、时延抖动超标）告警；要求提供功用截图并加盖厂商项目授权章 支持中文 WEB 界面管理及命令行管理，支持 SSH、HTTPS 的远程安全管理			
16	主机安全	系统架构 采用采集 C/S 模式，管理 B/S 模式架构；支持分散安装。 支持至少 5 种 Linux 64 位国际发行版，支持国产 64 位 Linux 操作系统，支持 Windows NT6.0 以上内核 64 位操作系统， 支持快速安装，支持指定分组安装；支持一键静默式安装；支持代理模式 Agent 管理 支持在线、离线、停用、删除 Agent 数据统计 Agent CPU 利用率小于 3%，内存使用率小于 80MB 可视化 支持分级视图、概览视图；支持视角切换 支持对单个主机整理详细数据，包括但不限于主机信息、硬件配置、系统账号、开放端口、运行进程、软件应用等 主机资产 支持对操作系统、主机类型、硬件配置、Agent 安装等信息进行清点 支持按照普通、重要、核心资产等级进行查询、筛选 进程端口 支持进程、端口清点，识别僵尸进程、等待进程 支持根据进程名识别常见应用和服务 系统账号 支持系统账号的发现、用户组、启用账号、禁用账号、登录信息等 支持根据登录时间、账号状态、账号名等进行查询、筛选	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		软件应用 支持 140 多种应用识别，支持应用名进行查询 支持自定义应用识别 Web 清点 支持 Linux 下的 Apache、Nginx、Tomcat、WebLogic、JBoss、WildFly、Jetty 应用服务，且显示详细路径 支持识别 300 多种 Web app 应用，支持 Web 站点检测，自动识别域名 支持自动识别 Web 框架开发语言，包括但不限于 PHP、JavaScript、Python、Java、.net 拓展信息管理 自动清点虚拟机内的安装包信息、启动服务信息、环境变量信息、内核模块信息； 未知资产检测 自动发现网络内存在的未知虚拟机，并可对网络检测速率进行自定义控制； 运维信息管理 可根据业务组、联系人、机房位置、设备编号等信息对服务器进行标注；并支持批量和自动标注； 数据库清点 支持 MySQL、Redis、MongoDB、MemCache、PostgreSQL、Hbase 等数据库的检测，包括但不限于版本、监听端口、配置文件路径、运行用户等 支持数据库名查询、筛选，显示数据库详情。 可视化 支持风险图形化展示，包含风险概况、风险分布、风险趋势、应用风险项统计、易受攻击列表、危急风险项、业务组风险项统计等 按风险项统计展示风险分析的过程和内容 安全补丁 支持清点主机中需要安装的安全补丁，根据补丁信息列出：补丁名称、危险程度、风险特征、影响主机数。 支持补丁的详细信息包括：补丁描述、验证信息、修复方法、基本信息、风险信息、参考信息 支持补丁修复条件和影响如：是否需要重启操作系统、影响的应用范围等。 弱口令检查 检测内容包括但不限于：弱密码账户、账号状态、密码值、弱密码类型、未修改密码天数。 支持 mysql、ssh、pptp、VNC、OpenVPN、rsync、Redis、vsftpd 等应用弱口令检测 支持自定义弱口令字典库，支持自动组合账号和口令字典，			

序号	名　称	技术参数要求	单位	数量	备注
		账号风险 自动清点并分析系统账号与用户组的情况，包含 root，sudo，key 使用状态，交互账号，启动账号，过期账号，密码锁定账号等多个维度的账号分析 应用风险 支持应用风险检查，包括但不限于 vcftp、redis、apache、apache2、mysql、ssh、ntp、rsync、nginx、mongoDB 等应用，检查结果包括：风险描述、验证信息、修复建议等 系统风险 支持检测系统存在的风险，例如 Grub 密码设置、路由转发、Ssh 协议版本检测、特定文件权限检查等 支持检测账号设置相关风险，例如 UID 重复、GID 重复、存在数字账号、Shadow 文件权限有问题等 反弹 shell 检测 支持实时发现黑客行为中反弹 shell 的入侵情况并及时告警通知。 提权检测 支持系统关键位置的权限诊断，详细列出系统存在的黑客提权行为的问题。 系统登录 支持实时监控系统登录情况，应支持黑、白名单机制监控系统登录，拦截暴力破解；支持自动将暴力破解 IP 加入黑名单。 后门检测 支持进行多层次 rootkit、bootkit 检测；支持已知特征检测、应用替换检测、后门目录文件检测、后门进程检测。 Webshell 检测 支持特征、文件相似度、沙箱多层次检测；应支持实时检测。			
	三、移动安全接入子平台				
（一）	网络资源				
1	互联交换机	整机 固化千兆以太网电接口≥48，上行万兆光接口数量≥4，满配业务扩展槽≥1，模块化双电源、模块化双风扇，配置 2 个万兆模块，含堆叠光模块 交换容量 ≥ 590 Gbps，包转发率≥250Mpps 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN 等功能，需提供官网选配信息截图证明，并加盖原厂项目授权章 功能 支持基于端口的 VLAN、基于 MAC 的 VLAN	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		支持 IPv4 静态路由、RIP V1/V2、OSPFv1/v2、OSPFv3、BGP4，BGP4+ for IPv6 支持基于协议 VLAN 支持通过 SFP 端口进行堆叠，最多支持 9 台设备堆叠； 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms； 支持 DHCP Snooping，防止欺骗的 DHCP 服务器 支持 ARP 检测来抵御 ARP 欺骗攻击； 产品资质 ▲为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；			
（二）	安全资源				
1	负载均衡	规格参数 机架规格 1U；单电源；不少于 6 个千兆电口，4 个千兆光口，1 个 RJ-45 Console 口，2 个 USB 口，硬盘≥64G SSD，内存≥8G；并发连接数≥800W，每秒新建连接数≥30W，最大有效吞吐≥10G；不少于 3 年设备原厂保修服务。 部署模式 支持路由、旁路部署，以及三角传输 高可用性 支持标准 VRRP 协议 N+1 集群部署：可以实现两台以上设备集群部署，多台设备同时负载一台设备在线备份，集群设备可以是不同的软件版本和型号 四层服务器负载均衡 支持轮询、加权轮询、最小连接、加权最小连接、静态就近性、动态就近性、全局可用、备选 IP、最小流量、最小带宽。 对于源，目的 IP 相同的 UDP 访问，可以对每个报文进行分类转发，保证流量负载的均衡性。 可以对 Radius 等接入认证服务器做基于用户的负载均衡，并且保证每个用户的请求分发到相同的服务器. 服务器过载保护：支持服务器每秒新建连接和会话数限制，保证分担任务不超过其负载能力。	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		支持通过 Vcenter 自动获取虚拟机状态，并将流量根据配置的负载均衡算法自动分配到各虚拟机。支持虚拟机管理，可监控虚拟机 cpu 占用率，内存占用率，健康状况，连接数等的状态；并根据以上条件对虚拟机进行关闭，挂起，重启，开启等操作。 7 层服务器负载均衡 通过应用层代理，可解析客户端请求内容， 并根据客户端请求头域做内容分发，将访问不同内容的请求代理到相应服务器上；并将响应数据代理到对应客户端。例如对图片类、文字类的请求，分别转发到对应的图片、文字服务器，支持基于 Cookie、User-Agent、URL、HTTP 头的分担模式。 服务器敏感信息保护：HTTP 头擦除、重定向信息改写、COOKIE 加密 设备接收到的 HTTP 流量时，可以按指定的规则对其内容进行管理，完成对出入的 HTTP 流量的检查、过滤、修改。主要包括：合规性检查、报文内容修改、重定向等功能。 支持 Http 协议重写，可以把 HTTP 请求自动重写为 HTTPS 协议，实现 HTTP 到 HTTPS 的无缝切换 全局负载 支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括 A ，NS，CNMAE，TXT，MX，PTR 记录。 支持 DNS 授权区域，可将 DNS 名称空间划分为区域来进行管理。可转发 DNS 请求，支持 forward-only forward-first 两种 DNS 转发模式。 支持地域优先、静态就近性、动态就近性 、基于权重、基于 session、基于服务器数量。 支持配置信息同步、状态信息同步。 基于 DNS 方式，在不同地域数据中心之间实现流量牵引。 界面及安全管理 支持全中文的管理界面和 HTTPS 方式登录 支持角色管理、多级授权管理。			
（三）	专用设备				
1	接入网关	基本要求：采用基于网络模式的 SSL VPN 技术，支持机构对机构连接、NAT 穿透、网络访问控制、B/S 应用、C/S 应用、多网关地址池集中管理等功能。支持 2 台以上(含 2 台)的移动 VPN 接入网关进行多机自负载均衡，无需添加专用的安全设备。加密数据传输与应用无关，有效支撑 B/S 和 C/S 应用。支持基	台	4	

序号	名　称	技术参数要求	单位	数量	备注
		于“数字证书”的认证方式，符合 X.509 证书格式，支持第三方 CA 认证。将状态信息纳入监控范畴，确保接入设备的可靠运行，并支持国密算法。 网络接口：≥6 个 10M/100M/1000M 自适应以太网接口； 加密速度：≥600Mbps/秒； 操作系统：采用安全的定制化的 Linux 操作系统； 算法要求：支持 SM1、SM2、SM3、SM4 国密算法； 性能要求：并发连接数≥5000；延时≤20ms;吞吐量≥800Mbps。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。 产品须满足现有海南全省公安移动终端（包括手持式移动警务终端和移动笔记本）用户平滑无缝对接使用要求，接入网关配套提供的安全客户端能够与现有用户密码卡产品兼容和适配，并提供相关证明材料。			
2	隔离网闸	基本要求：内、外网分别具有独立的管理接口，不是通过网络接口管理;内、外网分别具有独立的 HA 口，实现双机热备及负载均衡;内外网主机系统与专用隔离部件之间采用高性 PCI-E 总线连接，消除性能瓶颈;提供完善的日志审计;提供设备运行状态检测、系统资源监控。 硬件规格：2U 机箱，内外端机各≥6 个 10/100/1000Base-T(RJ-45)接口；系统吞吐量≥900Mbps；延时≤20us； 功能模块：功能模块：数据库同步、文件交换、数据库访问、邮件访问、安全浏览、安全 FTP、定制模块、工控访问等； 硬件架构：系统内部采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块；内外端机为网络协议终点，彻底阻断各种网络协议， 保证信任网络和非信任网络之间链路层的断开，彻底阻断 TCP/IP 协议以及其他网络协议。 网络能力 支持 IPv6	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。。			
3	移动应用管理系统	功能要求：移动应用管理系统与移动应用代理系统配合完成移动应用数据访问控制功能，在移动警务接入信息系统中，基于内外网信息安全隔离网闸，实现内外网信息系统之间的网络、数据及文件等信息的实时、非实时访问。基于主客体访问控制机制，对访问者（设备、服务、人员等）和被访问者（网络、数据、及文件等）进行标记和控制。同时提供系统访问日志审计功能。 基本规格：网络接口≥6 个 10/100/1000M 自适应以太网接口；最大新建连接数≥4000 次/秒；最大并发连接数≥5500；最大流量≥800Mbps；延时≤20us； 应用支持：支持 B/S 应用，http/https 协议。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。	台	2	
4	移动应用代理系统	功能要求：移动应用代理系统与移动应用管理系统配合完成移动应用数据访问控制功能，在移动警务接入信息系统中，基于内外网信息安全隔离网闸，实现内外网信息系统之间的网络、数据及文件等信息的实时、非实时访问。基于主客体访问控制机制，对访问者（设备、服务、人员等）和被访问者（网络、数据、及文件等）进行标记和控制。同时，提供系统访问日志审计功能。 基本规格：网络接口≥6 个 10/100/1000M 自适应以太网接口；最大新建连接数≥4000 次/秒；最大并发连接数≥5500；最大流量≥800Mbps；延时≤20us； 应用支持：支持 B/S 应用，http/https 协议。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。	台	2	
5	视频安全	功能要求：能支持视频组播；支持标准 SIP 协议,对于视频厂商实现了标准 SIP 协议的直接转发	台	1	

序号	名　称	技术参数要求	单位	数量	备注
	接入系统（前置）	支持标准 TCP/UDP 数据传输。对视频厂商实现了 TCP/UDP 代理协议转发。支持标准视频点播协议(H.264、H.263、RTSP），并可对协议进行分析和审核。 硬件规格：网络接口≥6 个 10M/100M/1000M 自适应以太网接口； 性能参数：最大并发连接数≥ 2000；最大流量≥800Mbps；支持≥400 路 D1 图象（2Mbps）或 100 路高清 8Mbps； 管理能力：采用基于 HTTPS 安全协议的管理方式；支持 SYSLOG、SNMPX 协议。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。			
6	视频安全接入系统（后置）	功能要求：能支持视频组播；支持标准 SIP 协议,对于视频厂商实现了标准 SIP 协议的直接转发 支持标准 TCP/UDP 数据传输。对视频厂商实现了 TCP/UDP 代理协议转发。支持标准视频点播协议(H.264、H.263、RTSP），并可对协议进行分析和审核。 硬件规格：网络接口≥6 个 10M/100M/1000M 自适应以太网接口； 性能参数：最大并发连接数≥ 2000；最大流量≥800Mbps；支持≥400 路 D1 图象（2Mbps）或 100 路高清 8Mbps； 管理能力：采用基于 HTTPS 安全协议的管理方式；支持 SYSLOG、SNMPX 协议。 网络能力 支持 IPv6 产品供应商需入围公安信息移动接入及应用系统安全设备厂商名录，并提供相关证明文件复印件，并加盖原厂商公章。	台	1	
7	视频网闸	功能要求：能支持视频组播；支持标准 SIP 协议,对于视频厂商实现了标准 SIP 协议的直接转发 支持标准 TCP/UDP 数据传输。对视频厂商实现了 TCP/UDP 代理协议转发。支持标准视频点播协议(H.264、H.263、RTSP），并可对协议进行分析和审核。 硬件规格：2U 机箱，内外端机各≥6 个 10/100/1000Base-T(RJ-45)接口，系统吞吐量≥900Mbps；延时	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		≤20us； 协议支持：支持 HTTP/HTTPS/FTP/SMTP/POP3 等应用协议;支持 H323/H323_GK 等多媒体协议；支持 SNMP/DNS 等网络协议； 视频编码格式支持：支持 M-JEPG，MPEG4、H.264、H.323 等编码格式； 视频分辨率：支持 D4、D1、VGA、2/3D1、1/1.8D1、SIF、3/4D1、CIF、QCIF; 硬件架构：系统内部采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块；内外端机为网络协议终点，彻底阻断各种网络协议， 保证信任网络和非信任网络之间链路层的断开，彻底阻断 TCP/IP 协议以及其他网络协议。			
8	网络探针	主要功能：采集公安内网所有设备的运行状态，包括 CPU、内存、网络等使用情况以及由操作系统产生的各类异常告警信息等；采集公安内网主要安全设备和业务系统的业务运行日志、管理员管理操作日志以及系统告警信息等；获取集中监管与审计系统、统一运维系统的管理参数，对公安内网网络设备的网络信息进行联动管理；支持与集中监管与审计系统的交互，获取对终端用户的管控策略；支持对采集的数据按照后台系统提供的规则进行数据清洗、抽取、分析，实现对用户流量、应用流量、应用访问频次的统计，并在此基础上对安全事件进行告警记录；支持与公安内网的统一运维系统对接，实现实时掌握设备状态，进行跨网版本升级、配置更新等统一维护操作。 协议支持：将通过 SYSLOG、v2/SNMP v3、Telnet、ICMP 等方式获取到的信息传输给内网集中监控管理系统；支持 SYSLOG、v2/SNMP v3、Telnet、ICMP 协议； 管理功能：使用基于 HTTPS 方式的管理设备； 稳定性运行时间(MTBF)：＞50000 小时； 网络接口：≥6 个千兆网络接口； 性能要求：吞吐量≥800Mbps；支持≥200 个采集单元。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。	台	1	

序号	名　称	技术参数要求	单位	数量	备注
	四、公安信息网服务子平台				
（一）	计算资源				
1	应用服务器	整机 机架式服务器，服务器高度≥2U，标配原厂导轨 CPU: ≥2 颗 Intel SP 6132，单颗核芯≥14 核,双线程，主频≥2.6GHz； 内存：≥256G DDR4 内存，频率≥2400MT，可扩展≥24 个内存插槽，最大支持最大容量 3.0TB 硬盘：≥8 个 2.5 寸热插拔硬盘槽位，≥ 2*600G 10K SAS，可扩展至≥40 个热插拔硬盘槽位，提供官网截图并加盖生产厂商项目授权章 网卡：≥2*10G SPF+ ，含模块；≥4*GE 电口； RAID 卡：≥1 个板载 专用插槽的 Raid 阵列卡，支持 Raid0/1/10/5，≥2GB 缓存，含断电保护 最多提供≥10 个 PCIE3.0 插槽（其中可支持≥3 个全宽高性能 GPU 卡），提供官网截图并加盖生产厂商项目授权章。 电源：本次配置 2 个≥500w 热插拔冗余电源，1+1 冗余电源 管理 配置≥1Gb 的远程管理控制端口,配置虚拟 KVM 功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟媒体等操作，提供服务器健康日记、故障现场还原，支持智能电源管理，支持服务器内部温度切面的 3D 显示，可支持动态功率封顶。 产品资质 ▲产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过 QC 080000 有害物质过程管理体系认证，提供证书复印件，并加盖原厂商公章或投标专用章 ▲为保证本项目的完善实施、严格按照要求落地，制造厂商均须具备良好的商业信誉，提供国家企业信用信息公示系统（网址：http://www.gsxt.gov.cn/）上行政处罚信息一栏的网站截图（带完整 URL 链接）证明，在“行政处罚内容“栏目内无行政处罚记录，并加盖厂商项目授权章；	台	25	
（二）	网络资源				

序号	名　称	技术参数要求	单位	数量	备注
1	互联交换机	整机 固化千兆以太网电接口≥48，上行万兆光接口数量≥4，满配业务扩展槽≥1，模块化双电源、模块化双风扇，配置 2 个万兆模块，含堆叠模块，配置可插拔防火墙硬件板卡一块 交换容量 ≥ 590 Gbps，包转发率≥250Mpps 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN 等功能，需提供官网选配信息截图证明，并加盖原厂项目授权章 功能 支持基于端口的 VLAN、基于 MAC 的 VLAN 支持 IPv4 静态路由、RIP V1/V2、OSPFv1/v2、OSPFv3、BGP4，BGP4+ for IPv6 支持基于协议 VLAN 支持通过 SFP 端口进行堆叠，最多支持 9 台设备堆叠； 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms； 支持 DHCP Snooping，防止欺骗的 DHCP 服务器 支持 ARP 检测来抵御 ARP 欺骗攻击； 产品资质 为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；	台	2	
2	数据存储交换机	整机 交换容量 ≥ 2.5 Tbps，包转发率≥1000Mpps 本次实配万兆光口≥48 个，40GE 光口≥2 个，业务扩展槽≥2 个，配置 48 个万兆多模光模块(850nm,300m,LC) 配置冗余双电源、冗余双风扇框，需提供官网截图和实物图片证明，并加盖原厂项目授权章 支持多种业务板卡扩展，支持 FW、IPS、防病毒、应用识别、SSL VPN、LB 等功能，需提供官网选配信息截图证明，并加盖原厂项目授权章，本次配置可插拔防火墙硬件板卡一块 功能 支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换 支持静态路由、RIP v1/2、OSPF、BGP 等动态路由协议，支持 RIPng、OSPF V3、IS-IS V6、BGP+ FOR IPV6、	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		IPV6 策略路由，支持 VRRP，支持等价路由支持基于端口的 VLAN、基于 MAC 的 VLAN 支持 VxLAN 集中式网关互通功能，支持 EVPN 分布式网关二三层互通功能 支持设备堆叠，最多支持 9 台设备堆叠 支持基于端口的 VLAN，支持基于协议的 VLAN 支持 IGMP v1/v2/v3，MLD v1/v2，支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2 支持 VRRPv2/v3（虚拟路由冗余协议），支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 200ms 产品资质 为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章；			
（三）	存储资源				
1	数据存储	整机 ▲多控制器架构，控制器之间采用 PCI-E 或 Infiniband 对等高速总线的全网状互连，多个控制器可以并行读写配置 4 个存储控制器，每个控制器之间通过 PCI-E 或 Infiniband 高速总线点对点对等互联，需提供厂商官网截图证明并加盖原厂项目授权章 ▲每个控制器配置 2 颗存储处理芯片，需提供厂商官网截图证明并加盖原厂项目授权章，控制指令和数据的传输通道物理分离，主控芯片也同样物理分离 配置 16Gbps FC 主机端口≥8 个，10Gb iSCSI 主机端口≥8 个 配置高速缓存≥128GB，缓存不包含 SSD 磁盘、PCI-E SSD、闪存、压缩或重删缓存和 NAS 控制器缓存 配置≥16 块 2.5″400GB SSD 企业级硬盘，≥16 块 2.5″1.8TB 10K SAS 企业级硬盘，≥36 块 8T 7.2K SAS 企业级硬盘 所有磁盘可同时配置为 RAID0/1/5/6，且可共存，支持无中断地 RAID 改变，支持多类型磁盘多方向、无中断在线数据迁移，迁移过程不影响业务性能 采用高速多对多磁盘故障恢复方式，提高恢复速度的同时，可保证磁盘复期间应用的性能，无专用指定热备盘，重建全局并发	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		配置硬盘扩展柜保护功能，当配置多个硬盘扩展柜时，可支持至少一个硬盘扩展柜掉电或故障时数据不丢失，应用不中断 存储功能 支持基于控制器的 SAN+NAS 软件授权，支持原生的 NAS 功能，无需另配 NAS 网关 从主机端口到硬盘全路径支持基于硬件的并符合业界标准的 T10-PI 数据一致性检测，保障数据的一致性，需提供厂商官网截图证明并加盖原厂项目授权章 配置图形界面管理软件，支持多种语言（至少包括简体中文和英文），支持多台设备集中管理，支持存储资源管理分析和资源使用历史记录分析，支持 WEB 管理，支持 CLI 管理。支持多种事件通知功能 配置自动精简、克隆、QoS、重删压缩、自动分层 配置性能监控和分析软件，配置高级图形化报表软件，可以定制历史运行数据的图形化报表 支持将快照直接备份到二级存储或者服务器上，支持二级存储/服务器上所备份的快照恢复到原磁盘阵列或其他磁盘阵列 支持存储远程复制功能，支持与同厂商高端型号以及全闪存阵列间实现存储底层复制，包括远程复制和可在线迁移卷 支持存储双活功能，在不加额外网关的情况下可以实现和同厂商高中端型号存储组成双活阵列，在一台阵列故障的情况下，主机 IO 访问可以无缝切换到另外一台阵列而不会中断业务 在不加额外网关的情况下可以实现和同厂商的高中端存储和全闪存存储组成存储集群，数据可以在多台存储之间按照性能、容量等策略进行在线数据迁移，对于主机平台透明 产品资质 投标产品必须为成熟产品，并需提供官方 6 个 9 的高可用证明并盖原厂项目授权章			
2	备份存储	整机 要求与存储设备同品牌；可与现有的备份应用和流程实现无缝集成，专用磁盘备份设备，非虚拟带库网关架构 配置处理器≥2 颗，≥8 核 配置高速缓存≥128GB 配置≥4 个 10Gb 以太网接口	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		配置≥12 块 4TB 7200 转 SAS 硬盘，备份可用的数据磁盘存储可用容量≥31.5TB，最大扩展可用容量可达 108TB 采用 RAID 6 保护；支持热插拔硬盘、冗余电源、风扇等 单台设备可虚拟的磁带库及 NAS 数量≥36 支持模拟的磁带格式为 LTO-4、LTO-5，LTO-6 和 LTO-7 等 备份目标方式 支持 NAS、VTL 和 Symantec OST 三种备份目标方式 NAS 备份目标要求支持 NFS 和 CIFS 要求 iSCSI 环境下支持 VTL 备份目标方式 本次要求配置 VTL,NFS,CIFS,OST 功能 存储功能 提供在线重复数据删除技术，提供磁盘备份设备之间的低带宽数据复制许可 采用可变长数据块重复数据删除，提高重复数据删除效率 配置无限容量许可的中文图形化虚拟带库管理软件，可以通过一个管理软件管理多台虚拟带库设备 支持将备份设备直接作为 Oracle RMAN 目标进行 Oracle 备份 支持将备具备自动管理、自动配置、自动监控及性能调试等功能，可通过简单的界面进行轻松安装份设备直接作为 SQL 目标进行 SQL 备份 支持将备份设备直接作为 Exchange 目标进行 Exchange 备份 支持并包含将主阵列的快照备份到本设备，并且将快照恢复到原始阵列或者其他相同快照格式阵列			
（四）	软件				
1	备份软件	授权许可 备份软件本次配置 16TB 前端容量授权，包含所有的备份功能 为便于存储业务管理及兼容性，要求备份软件与数据存储、备份存储同一品牌 功能 支持主流 UNIX、Linux 和 Windows 与 OpenVMS、Mac OS X Server、Novell、Sun Solaris (SPARC)、Sun Solaris (x86 and x64)、HP-UX (Itanium & PA-RISC)、AIX、SCO OpenServer、RHEL、SLES、CentOS、Debian、Ubuntu、Scientific Linux	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		支持 SAP HANA、SAP R3、SAP MAXDB、MYSQL、PostgreSQL、Oracle、Sybase、DB2、SQL Server、Informix、Exchange、Domino 等数据库；对以上数据库的集成备份，无需借助第三方工具或定制脚本。 无限制标准客户端与企业客户端的许可，并提供客户端推送安装功能，降低认为误操作或者实施成本，提供功能截图证明并加盖原厂项目授权章 提供系统灾难恢复能力，可以在发生灾难后将整个系统（包括操作系统、驱动程序、应用系统）快速恢复到最近备份时间点配置 备份软件支持安装在主流的操作系统平台上，主要有：UNIX、WINDOWS、LINUX 平台 要求提供中文管理界面，提供方便灵活的全图形化工具来完成备份、恢复、定制、监控等操作，无需编写任何脚本即可完成数据库的备份和恢复操作 对 Oracle 数据库进行备份和恢复时提供全图形化操作,尤其针对 oracle 数据库恢复时，无需手工编写 RMAN 脚本或者在客户端中执行 RMAN 恢复命令。统一通过恢复的 GUI 界面，完成恢复，并支持开启 oracle 数据库，支持 Oracle CDB 与 PDB 模式备份，需提供产品截图并加盖原厂项目授权章 备份文件采用统一专有格式，记录了备份信息的标签和日志信息，保证备份内容的安全性， 支持灵活备份策略的定制，支持备份策略的暂停功能 软件提供备份重复数据删除功能，缩短备份时间，备份软提供源端、服务器端或目标端等多种方式重复数据删除功能 备份软件可以结合虚拟带库实现数据源端重复数据删除，备份软件在源端进行重复数据删除以后，直接通过低带库数据传输给虚拟带库，虚拟带库无需再进行重复数据删除，支持虚拟带库的全局重删技术，并支持虚拟带库作为磁盘介质备份 支持多个备份域环境的统一管理，简化备份操作，实现统一监控与备份管理 配置客户端推送安装功能，同时添加卸载客户端/管理服务器，任何系统都不需要重启，降低认为误操作或者实施成本			
（五）	安全资源				

序号	名　称	技术参数要求	单位	数量	备注
1	集中管控日志服务器	整机 配合探针收集、汇聚各类系统的部署、运行情况，并与平台关键节点联动，部署数据库集群，可以虚拟化部署 机架式服务器，服务器高度≥2U，标配原厂导轨 CPU: ≥2 颗 Intel SP 4110，单颗核芯≥8 核,双线程，主频≥2.1GHz； 内存：≥8*16G DDR4 内存，频率≥2400MT，可扩展≥24 个内存插槽，最大支持最大容量 3.0TB 硬盘：≥25 个 2.5 寸热插拔硬盘槽位，≥ 10*1.2T 10K SAS，可扩展至≥40 个热插拔硬盘槽位，提供官网截图并加盖生产厂商项目授权章 网卡：≥4 个 10/100/1000M-BaseT 以太网接口； RAID 卡：≥1 个板载 专用插槽的 Raid 阵列卡，支持 Raid0/1/10/5，≥2GB 缓存，含断电保护 最多提供≥10 个 PCIE3.0 插槽（其中可支持≥3 个全宽高性能 GPU 卡），提供官网截图并加盖生产厂商项目授权章。 电源：本次配置 2 个≥500w 热插拔冗余电源，1+1 冗余电源 管理 配置≥1Gb 的远程管理控制端口,配置虚拟 KVM 功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟媒体等操作，提供服务器健康日记、故障现场还原，支持智能电源管理，支持服务器内部温度切面的 3D 显示，可支持动态功率封顶。 产品资质 产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过 QC 080000 有害物质过程管理体系认证，提供证书复印件，并加盖原厂商公章或投标专用章 为保证本项目的完善实施、严格按照要求落地，制造厂商均须具备良好的商业信誉，提供国家企业信用信息公示系统（网址：http://www.gsxt.gov.cn/）上行政处罚信息一栏的网站截图（带完整 URL 链接）证明，在“行政处罚内容“栏目内无行政处罚记录，并加盖厂商项目授权章；	台	3	
2	负载均衡	规格参数 机架规格 1U；单电源；不少于 6 个千兆电口，4 个千兆光口，1 个 RJ-45 Console 口，2 个 USB 口，硬盘≥64G SSD，内存≥8G；并发连接数≥800W，每秒新建连接数≥30W，最大有效吞吐≥10G；不	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		少于 3 年设备原厂保修服务。 部署模式 支持路由、旁路部署，以及三角传输 高可用性 支持标准 VRRP 协议 N+1 集群部署：可以实现两台以上设备集群部署，多台设备同时负载一台设备在线备份，集群设备可以是不同的软件版本和型号 四层服务器负载均衡 支持轮询、加权轮询、最小连接、加权最小连接、静态就近性、动态就近性、全局可用、备选 IP、最小流量、最小带宽。 对于源，目的 IP 相同的 UDP 访问，可以对每个报文进行分类转发，保证流量负载的均衡性。 可以对 Radius 等接入认证服务器做基于用户的负载均衡，并且保证每个用户的请求分发到相同的服务器. 服务器过载保护：支持服务器每秒新建连接和会话数限制，保证分担任务不超过其负载能力。 支持通过 Vcenter 自动获取虚拟机状态，并将流量根据配置的负载均衡算法自动分配到各虚拟机。支持虚拟机管理，可监控虚拟机 cpu 占用率，内存占用率，健康状况，连接数等的状态；并根据以上条件对虚拟机进行关闭，挂起，重启，开启等操作。 7 层服务器负载均衡 通过应用层代理，可解析客户端请求内容， 并根据客户端请求头域做内容分发，将访问不同内容的请求代理到相应服务器上；并将响应数据代理到对应客户端。例如对图片类、文字类的请求，分别转发到对应的图片、文字服务器，支持基于 Cookie、User-Agent、URL、HTTP 头的分担模式。 服务器敏感信息保护：HTTP 头擦除、重定向信息改写、COOKIE 加密 设备接收到的 HTTP 流量时，可以按指定的规则对其内容进行管理，完成对出入的 HTTP 流量的检查、过滤、修改。主要包括：合规性检查、报文内容修改、重定向等功能。 支持 Http 协议重写，可以把 HTTP 请求自动重写为 HTTPS 协议，实现 HTTP 到 HTTPS 的无缝切换 全局负载 支持标准 DNS 服务器功能，支持多种 DNS 记录 ，包括 A ，NS，CNMAE，TXT，MX，PTR 记录。			

序号	名　称	技术参数要求	单位	数量	备注
		支持 DNS 授权区域，可将 DNS 名称空间划分为区域来进行管理。可转发 DNS 请求，支持 forward-only forward-first 两种 DNS 转发模式。 支持地域优先、静态就近性、动态就近性 、基于权重、基于 session、基于服务器数量。 支持配置信息同步、状态信息同步。 基于 DNS 方式，在不同地域数据中心之间实现流量牵引。 界面及安全管理 支持全中文的管理界面和 HTTPS 方式登录 支持角色管理、多级授权管理。			
（六）	专用设备				
1	集中管控中心	规格：通用服务器部署，网络接口：≥4 个千兆网络接口。 性能要求：吞吐量≥800Mbps。 协议支持：支持 Syslog、SNMP、WebService 等标准协议。 资源管理：汇聚各区域全要素数据，包括用户、数字证书卡（绑定身份证书）、终端、服务器主机、网络设备、通用和专用安全设备、应用等资产进行信息展示与维护。 统计分析：对各区域安全管控系统上报的用户、终端、应用、主机、网络设备、安全设备等信息以及安全事件信息进行统计。需按不同时间段，不同机构，不同警用，不同部署区域，不同类型等进行多维度统计，并为可视化展示奠定数据基础。 监测审计：以区域安全管控系统上报的各要素日志为数据源，对日志进行监测审计、关联分析和实时的运维监测、安全监测。 集中展示：将统计分析的多维度数据和监测审计的实时数据，进行集中的数据可视化展示。展示方式分为两种：态势展示和控制台展示。态势展示会将移动警务平台关键数据以动态形式呈现，控制台展示可以对数据进行链接、索引。 安全管理：针对用户、终端、网络、数据、应用定义其相应的安全策略及联动管控策略，需区分运维策略、安全策略，实现对安全事件和运维时间的响应。	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		部省级联：按照公安部集中管控全国级联要求，完成级联工作。 产品按照《全国公安移动警务建设总体技术方案(2016 版)》要求，须确保能与部级移动警务平台及时完成无缝对接级联，提供相关证明材料进行说明。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。。			
2	网络探针	主要功能：采集公安内网所有设备的运行状态，包括 CPU、内存、网络等使用情况以及由操作系统产生的各类异常告警信息等；采集公安内网主要安全设备和业务系统的业务运行日志、管理员管理操作日志以及系统告警信息等；获取集中监管与审计系统、统一运维系统的管理参数，对公安内网网络设备的网络信息进行联动管理；支持与集中监管与审计系统的交互，获取对终端用户的管控策略；支持对采集的数据按照后台系统提供的规则进行数据清洗、抽取、分析，实现对用户流量、应用流量、应用访问频次的统计，并在此基础上对安全事件进行告警记录；支持与公安内网的统一运维系统对接，实现实时掌握设备状态，进行跨网版本升级、配置更新等统一维护操作。 协议支持：将通过 SYSLOG、v2/SNMP v3、Telnet、ICMP 等方式获取到的信息传输给内网集中监控管理系统；支持 SYSLOG、v2/SNMP v3、Telnet、ICMP 协议； 管理功能：使用基于 HTTPS 方式的管理设备； 稳定性运行时间(MTBF)：＞50000 小时； 网络接口：≥6 个千兆网络接口； 性能要求：吞吐量≥800Mbps；支持≥200 个采集单元。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。	台	1	
3	数据探针	功能要求：采集所在区域业务数据，按照过滤策略进行敏感数据报警、接收数据副本功能； 数据清理后进行上报集控中心。 协议支持：SYSLOG、v2/SNMP v3、Telnet、ICMP；	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		管理功能：使用基于 HTTPS 方式的管理设备； 稳定性运行时间(MTBF)：＞50000 小时； 网络接口：≥6 个千兆网络接口； 性能要求：吞吐量≥800Mbps；支持≥200 个采集单元。 稳定性 为确保系统稳定性，网络探针、数据探针、安全管控系统、集中管控中心为集中管控专用设备，要求为同一品牌，提供相关证明材料。			
4	安全认证管理系统	密码能力 内置安全密码机，可以创建一对公私密钥对，以此作为整个 PKI 体系的可信根 发证能力 支持国密 SM2 证书签发。 证书 管理能力 基于公安信息网 PKI 技术的数字证书身份认证方式提供对数字证书的审核、签发、管理、撤销等。 审计能力 提供日志管理和集中管控 用户数 不少于 3 万 认证能力 每秒不少于 200 个 签发证书 能力 不少于 20 张/秒 网络能力 机架式设备，不少于千兆网口×4，支持 IPv6 兼容性要求 为保证系统兼容性，需与接入网关为同一品牌，提供相关证明材料。	台	1	
5	智能移动终端管理（MDM 系统）	总体管控方案 提供一套完整的多模式警务终端安全管控方案，包含多模式警务终端安全管控平台。要求安全监控组件内置于多模式警务终端，对一台终端上的生活模式和工作模式分开管理，能够实现基本管理、设备管理、网络管理、通话管理、多模式管理、应用管理、安全管理等功能。 按照《全国公安移动警务建设总体技术方案（2016 版）》规定，针对可访问互联网的Ⅰ类系统，移动智能终端生活模式下可以安装移动警务Ⅰ类系统应用，以及个人所需要的软件，提供终端互联网使用便利。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		在此类场景中管控平台对终端提供必须的辅助管理功能： 1）移动智能终端丢失后可以提供安全管控策略，对终端进行锁机或全终端数据销毁； 2）与管控平台同步系统时间，同时禁止修改普通系统的系统时间； 3）发生工作 SIM 卡和安全 TF 卡拔出、更换等异动，立即对终端进行锁机或全终端数据销毁； 4）禁止终端在 I 类系统中手工配置工作的 APN 参数； 5）禁止终端在 I 类系统中热点共享工作用的 APN 接入点。 针对Ⅱ类、Ⅲ类安全系统，智能终端运行在工作模式下，将完全运行内部移动警务应用，同时需满足如下管控要求： 基本管理 终端启用 1、预注册：由管理员在后台通过单个或批量方式导入用户信息和终端 IMEI、SIM 卡 IMSI 等信息。 2、终端激活：终端插入 SIM 卡，通过扫描注册二维码，并通过后台导入的用户信息、SIM 卡(IMSI)等验证后，进行关联绑定，并且激活。 3、机卡绑定：管控平台根据终端注册时使用的终端号卡与终端进行一对一绑定。当终端上使用的号卡发生变化时，对终端进行异常行为监管，锁定终端，防止终端的违规使用 终端退役 1、终端丢失：终端发生丢失时支持擦除终端数据并解除人员、终端、SIM 卡绑定关系。 2、终端注销：支持注销终端管理，注销后终端解除管理状态，清空管理指令。 3、终端解绑：通过管理员操作系统后台对原先绑定的终端解除绑定，为人员替换或更换终端、号卡时提供业务服务。 设备管理 1、终端端口管理（开启/关闭）：系统后台可以控制终端上相关端口功能的开启和关闭，包括：蓝牙开启/关闭、摄像头开启/关闭、麦克风开启/关闭、网络访问开关（WIFI 开启/关闭、移动数据开启/关闭）、个人热点开启/关闭、GPS 开启/关闭、USB 调试和 USB 大容量存储功能开启/关闭、SD 卡功能开启/关闭，飞行模式功能开启/关闭，截屏功能开启/关闭，录屏功能开启/关闭			

序号	名　称	技术参数要求	单位	数量	备注
		2、终端资产管理：显示终端基本信息，包括：终端号码、用户名称、所属部门、终端状态、是否在线、是否 Root、是否外出、是否失联、最后连接时间等信息。 3、端到端管理：管理员可以通过终端对自己管理权限范围内的终端进行管理，包括锁定终端、寻找终端、盘点终端、发送消息等各项功能。 、远程协助：管理员通过系统后台对终端发起远程协助，终端接受许可后，管理员在管控 PC 上可以远程接管该终端安全工作模式的界面，针对终端使用的问题，提供远程协助，远程帮助终端使用者解决问题。 5、终端文件管理： 终端文件获取：要去系统能够通过后台获取终端存储空间指定目录中的文件。 终端文件推送：要求系统能够通过后台对终端存储空间的指定目录中推送文件。 6、离线管理：当终端初始化以及在线的情况下接收到管控后台下发的管控指令和策略后，即使终端处于离线状态下，被预先设置的管控指令和管理策略仍然生效：例如执行锁屏、应用黑白名单管控、应用安装限制、热点分享、限制使用蓝牙、限制使用 USB、限制使用 GPS 等管理。 7、时间围栏：可配置时间围栏的管理动作，当终端到达设定的时间自动触发执行时间围栏配置的管理。 #8、禁止修改终端时间：禁止用户手动修改终端的系统时间，并且可以强制终端与后台的时间基准服务器进行时间同步。 9、地理围栏：可配置地理围栏的管理动作（围栏内或者围栏外），当终端在指定的地理位置时自动触发执行地理围栏配置的管理。 10、离线地图定位：使用离线地图方式，实现内网定位。 11、策略执行跟踪：在策略分配后，可在后台查看策略执行情况：查看策略分配任务执行列表（策略名称、执行人、执行时间）；点击单行展示指令总数、未执行数、已执行数、取消数；终端执行列表明细查看、导出。 12、终端管理状态查询：管理员通过系统后台查询所有注册终端的已注册、在线、失联、外出、Root、			

序号	名　称	技术参数要求	单位	数量	备注
		已注销等管理状态。 13、蓝牙配对白名单：白名单内的蓝牙设备，终端允许连接，白名单外的蓝牙设备，终端禁止连接 14、WiFi 热点白名单：管控服务平台配置终端 WiFi 热点白名单，终端打开热点之后，仅白名单中的设备可以连接该热点，其他设备无法连接。 网络管理 1、强制开启移动数据：为防止终端与服务器中断链接而脱管，系统可以下发指令强制终端开启移动数据。 2、移动数据卡槽管理：办公模式强制使用工作卡移动数据。生活模式优先使用工作卡移动数据，用户可选择使用个人卡移动数据。 3、专用 APN/VPDN 自动配置和接入：APN/VPDN 配置信息通过系统后推送，终端自动配置和切换到接入网 APN/VPDN，并且保证接入网 APN/VPDN 配置不可修改，且一直处于保活状态。 4、接入网的 APN/VPDN 批量生成：系统后台支持接入网 APN/VPDN 配置的批量生成。 5、VPN 管理：后台可以配置 VPN 菜单禁用/启用（设置-移动网络-VPN），可以禁用/启用对 VPN 的保活；后台配置 VPN 客户端属性，根据属性自动下载和安装 VPN 客户端。 6、VPN 自动接入：支持在接入网 APN/VPDN 切换成功后，可以自动调用拨通 VPN，并且保活 VPN 连接。 7、禁止网络热点共享　禁止通过 USB 网络分享、蓝牙网络分享以及热点分享功能，防止通过共享网络非法接入内部网络。 通话管理 1、通话功能限制：后台可以控制终端的通话功能的使用，当限制通话功能时，终端不能接听与拨打电话。 双模式管理 为保证用户内部应用和数据的安全性，系统要求支持多模式管理，将生活模式和工作模式分别进行管理，对多模式管理的主要功能如下： 1、登陆认证：终端进入工作模式时，要求输入工作模式密码，同时要求支持三个认证一次性拨通：VPDN，安全链路长链接，TF 卡加密认证，只有通过认证才可以访问工作模式。 2、工作模式管理：工作模式中的数据以加密形式存储，只能被指定的工作模式中的应用打开或访问，			

序号	名　称	技术参数要求	单位	数量	备注
		禁止工作模式外的应用访问安全容器中的数据。 3、工作模式应用管理：系统支持工作模式专有 App 的上传、审批、下发、安装（静默安装和手动安装）、卸载（静默卸载和手动卸载）、更新（静默更新和手动更新）功能。 4、工作模式网络连接：工作模式通过 APN/VPDN 链路接入，默认禁止 WiFi 数据连接。 5、工作模式锁定/解锁：系统支持在设备出现异常的情况下远程锁定工作模式，使工作模式无法被访问，当确定设备正常后解除锁定。 6、工作模式擦除：系统支持对工作模式远程擦除。 7、控制破解设备对应用的访问：如设备被破解禁止使用指定的应用，工作模式自动被擦除； 8、控制应用数据的拷贝、剪切和粘贴：工作模式内外无法以剪切、复制和粘贴的方式传输数据。 9、超时登陆：工作模式登录后如果长期在线不使用，再次使用时，用户需要重新登录。 10、应用隔离：工作模式中的应用只能在相应的工作模式中的被打开或访问，禁止被普通工作模式应用访问。 11、数据隔离：生活模式与工作模式中的通话记录、通讯录、图片、视频、应用数据以及其他信息不能互相访问。 12、全设备擦除：管控平台支持远程同时擦除生活模式、工作模式以及 TF 卡数据。 #13、多模式端管控指令分区生效：系统可以对多模式分别制定指令策略，并指定下发给终端不同模式，并在该模式下生效，当终端进行模式切换时，自动生效切入模式的管控策略。 应用管理 1、应用白名单：系统后台支持应用白名单库，支持增、删、改、查、导入操作，安全监控组件仅允许白名单中的应用可以下载安装并使用，禁止终端使用白名单外的应用。 2、应用黑名单：系统后台支持应用黑名单库，支持增、删、改、查、导入操作，安全监控组件禁止安装和使用黑名单中的应用。 3、应用安装功能限制：系统后台可以控制终端安装应用功能的使用，当限制安装功能时，终端上所有的软件安装包均无法安装（包括通过互联网下载、存放在 SD 卡上、通过蓝牙/红外传输、与电脑 USB 连			

序号	名　称	技术参数要求	单位	数量	备注
		接拷贝安装包）。 4、应用防卸载：禁止用户卸载终端上的应用，包括自带应用和手动安装的第三方应用，可以指定保护某一程序不被卸载。 5、应用静默/强制安装接口：为应用商店提供接口可通过服务器管理端对移动终端下发策略实现应用静默/强制安装。 6、禁用/允许系统自带应用商店：禁止/允许使用系统自带应用商店。并且禁止 USB、TF 卡、下载等其他应用安装途径。 7、软件资产管理：可在终端上查看应用的详细信息，包括：软件名称、包名、版本号、软件大小、是否系统应用、是否白名单应用、安装时间、上报时间等。 安全管理 1、终端锁机：系统后台可以对终端进行远程锁定，锁定后无法正常使用终端的各项功能，包括拨打、接听电话，发送短信等。 2、修改密码：支持对单台、多台终端修改系统锁屏密码。 3、清除密码：支持对单台、多台终端清除系统锁屏密码。 4、离线密码：后台提供一套算法生成动态离线密码，以避免网络无法连接导致终端锁定后无法解锁。 5、设备级水印：要求系统提供设备级水印，根据需求能够给指定应用或者全设备加载水印。 6、终端异常管理： ROOT：当检测到终端被 Root 后，终端将进行锁机、擦除等等管理。 失联：当检测到终端失联后，终端将进行锁机、擦除等等管理，且管理指令无论是在网或者离线状态下都会生效执行。 7、终端擦除/恢复出厂设置：系统后台可以对单台、多台终端擦除终端数据，将终端恢复出厂设置。 人员组织管理 1、组织维护：系统后台支持分级管理，对部门的增、删、改、查、批量导入。 2、人员维护：系统后台支持人员的增、改、查、批量导入，绑定人员和 IMSI 信息。 3、人员管理：基于一体化平台提供的人员架构进行部署，如果人员调动了，自动推送人员当前部门相			

序号	名　称	技术参数要求	单位	数量	备注
		关应用并删除之前部门不相关应用。 4、分组管理：除了可根据组织机构的方式进行管理外，后台还可为根据管理要求创建不同的人员分组，通过分组进行策略管理。 系统管理 1、权限管理：后台可创建多个管理员，对管理员可管理的组织机构范围进行设定，从而提供不同权限的管理账户。 2、角色管理：系统后台通过不同管理功能的配置将管理员进行角色化区分。 3、管理员管理：系统后台可对管理员进行增、删、改、查、角色分配，并且支持多级管理员管理结构，上级可管理下级，不可管理与查看上级或平级。 4、修改管理员密码：修改管理员系统登录密码。 系统监控 1、 已注册数：统计当前管理范围内已注册终端数量。 2、 在线数：统计当前管理范围内在线的终端数量。 3、 越狱数：统计当前管理范围内被 Root 的终端数量。 4、 失联数：统计当前管理范围内离线时间超过设置的失联时间的终端数量。 5、 日新增终端量统计图：以折线图形式展示一周内管理范围内每日新注册终端情况。 6、 日指令发送量折线图：以折线图形式展示一周内管理范围内管理员每日发送指令总数情况。 7、 终端失联监控：实时显示管理范围内的失联终端记录。 可视化监控：要求提供监控指挥中心实时展示终端情况和违规情况，以及人员热力分布图。 报表管理 1、 终端报表：支持终端离线、ROOT、失联（包含失联时间配置小时展示）的查询及导出 2、 限制状态报表：终端限制情况查询分析。展示当前终端蓝牙、摄像头、麦克风、WIFI、移动数据的限制情况。 3、 应用报表：汇总终端上应用的安装情况，按照应用的安装量降序展示，可查看应用的详细安装信息，包括应用名称、包名、版本名称、是否系统应用、终端 ID、终端号码、用户名称、所属部门，支持报表导出功能			

序号	名　称	技术参数要求	单位	数量	备注
		4、 流量统计报表：统计应用的使用时长和移动数据流量使用 5、 管理员日志报表：记录管理员的操作日志，支持查询和导出报表 6、 安全监控组件客户端自更新统计：查询统计安全监控组件客户端新版本的更新情况 外部接口 1、单点登录：系统需提供第三方应用统一登录接口，供第三方应用登录认证。在用户登录移动门户后，可直接在门户中启动第三方应用，而不需要二次登录。 2、为第三方应用提供保活接口：提供第三方应用的保活机制，防止第三方应用在息屏、低电量模式下被系统杀掉进程和服务。 强壮性要求 1、安全监控组件防卸载：要求支持安全监控组件卸载保护机制，用户在界面上无法卸载安全监控组件客户端，管理员卸载客户端应用程序需要通过输入卸载密码或通过管理中心指令卸载。 2、安全监控组件系统权限保活：在终端厂商自带的终端管家中取消安全监控组件的权限，这些权限不能被取消；系统清理内存模式下、低电量模式下安全监控组件进程依然保活 3、软恢复出厂管理：禁止从终端设置界面中恢复出厂； 、硬恢复出厂管理：终端被硬键组合开机后恢复出厂依然被管控； 5、防 ROOT：终端被 ROOT 后立即被锁机或者被擦除； 6、防刷机：终端无法被刷机后脱离管控或挪为他用。 管理平台技术性能参数 在安全接入平台环境下运行，对性能有如下要求： （1）要求系统能够承载管理≥5000 台设备，且能够根据实际需要进行线性扩容； （2）终端管理平台服务器支持并发用户数≥500； （3）实时管控命令反馈：≤5 秒； （4）主动检测巡检时间：≤30 分钟。 资质要求 1.投标人需提供由公安部门颁发的多模终端安全管控系统信息安全等级保护三级及以上认证备案证书，提供证书复印件并加盖厂商公章或投标专用章； 2.投标人所投平台需提供由公安部监制的计算机信息系统安全专用产品销售许可证，提供证书复印件并			

序号	名　称	技术参数要求	单位	数量	备注
		加盖厂商公章或投标专用章； ▲3.投标人所投平台需提供由中国网络安全审查技术与认证中心颁发的 ISCCC IT 产品信息安全认证证书，提供证书复印件并加盖厂商公章或投标专用章； 4、投标人所投平台需通过 ISO27001 信息安全管理体系认证，提供证书复印件并加盖厂商公章或投标专用章； 5、投标人所投平台需通过 ISO9001 质量管理体系认证，提供证书复印件并加盖厂商公章或投标专用章；			
6	NFC 解码设备	网络接口： 12 个电口 机箱大小：标准 2U 身份证解码服务器功能 1) 网络解码设备不带硬盘，确保不存储身份证信息。 2)支持 1200 个终端用户进行身份证联网请求 3)身份证识别速度小于 5 秒，每百次成功率 90%以上 4)高性能传输协议，避免因网络抖动产生读卡失败问题 5)采用高性能芯片确保芯片与解码模块的高速运算提高读卡成功率 6) RSA+AES 算法配合动态秘钥技术，实现解码数据安全传输。	台	2	
7	网络流量分析系统	整机 2UX86 服务器架构，冗余双电源； 双 Intel E5-2630v4 CPU 或以上,共 20 个物理核以上；内存 64GB、硬盘容量 44TB 以上，配置硬件 2G 缓存 RAID 卡; 配置≥2 个万兆 SFP+光口,≥4 个千兆电接口 最大流量处理能力 20Gbps，最大报文存储性能 10Gbps，最大并发用户数 10 万， 最大并发会话数 400 万，最大新建会话数 20 万/秒 功能 基于 B/S 架构进行管理和流量数据分析，能够分布式部署在各个监控的网络节点，实时分析捕获流量,实时保存捕获到的网络通讯数据包，进行长时间、大容量的数据存储能力	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		▲采用软硬件一体化设计，通过 WEBUI 直接进行流量回溯、流量可视化的查看、搜索；要求提供功用截图并加盖原厂项目授权章 支持交换机镜像、路由器镜像、分光器、网络分流器等部署方式，支持以太网、POS 接口流量镜像分析，旁路部署，对网络整体架构无影响 支持离线报文远程解码分析，支持源端回溯系统存储报文通过 WEB 进行协议解码（不需要下载到本地）、时序图展示、HTTP 等内容还原；要求提供功用截图并加盖厂商项目授权章 能够实时捕获并保存网络中的通讯数据包，存储时间可以根据硬盘大小进行调整 能实时分析并长期保存网络中的所有数据流统计数据，包括详细的 IP 会话流、TCP 会话流、UDP 会话流数据，数据精度到秒级，数据流统计数据要求能保存至少 1 个月； 支持基于 1 秒、10 秒、1 分钟、10 分钟几种颗粒度进行回溯展示； 支持在线用户、用户历史流量、用户实时流量、用户中心展示，可以查看用户终端、用户虚拟画像、用户与应用流量的二级钻取；要求提供功用截图并加盖原厂项目授权章 支持应用的实时流量、历史流量、应用质量、未知应用可视化呈现、展示 支持服务器的实时流量、会话统计，支持服务器历史流量会话统计，支持单个服务器下的用户流量、会话统计；要求提供功用截图并加盖原厂项目授权章 支持行为呈现的数量趋势图、各行为类型分布饼图、以及各行为的表格数据，各行为可以二级钻取，查看 TOP10 的排名以及 TOP10 用户访问; 视频监控网络质量进行分析，分析流量、流量突发、网络丢包、网络时延、网络抖动等业务指标，针对摄像头、业务服务器进行质量排名；要求提供功用截图并加盖原厂项目授权章 支持视频监控网络流量异常（流量中断、突发、时延抖动超标）告警；要求提供功用截图并加盖厂商项目授权章 支持中文 WEB 界面管理及命令行管理，支持 SSH、HTTPS 的远程安全管理 产品资质 投标产品生产厂商需具备科学、系统的知识产权管理体系。能够全面保护、并系统管理知识			

序号	名　称	技术参数要求	单位	数量	备注
		产权，支撑企业的技术创新能力。投标产品供应商必需通过知识产权管理体系认证，提供知识产权管理体系认证证书，并加盖厂商项目授权章；			
（一）		警员 PKI/PMI 系统国密算法升级			
1	CA 系统	功能 核心架构换代，将原有 C/S 架构换代为 B/S 结构。 系统应具有对 SM2 算法体系支持，包括 CA 签名证书密钥算法、用户证书密钥算法、服务器证书密钥算法、管理员证书密钥算法。 系统应支持基于双算法的证书申请、下载、更新、冻结、解冻、注销证书等功能。 系统应支持国产操作系统、数据库和服务器。 系统应支持归档证书的存储，确保归档证书信息的完整性和易用性。 系统应提供 CRL 服务，具有黑名单管理功能，可以同步 CRL 至 LDAP，黑名单发布模式应支持但不限于增量 CRL 和全量 CRL 的发布模式。 系统应支持 CA 策略管理功能，可以为 CA 证书制定不同的策略，配置策略应包括但不限于管理员证书的策略配置、个人 RSA/国产密码双证书的策略配置、设备证书的策略配置、域控制器证书的策略配置。各类型证书策略配置模板应包括但不限于证书有效期的配置和密钥用法的配置。 系统应具有 CA 证书管理的功能，主要包括查询、生成、导出、导入、取消和撤销功能并且应具有对下级 CA 进行签发、查询、废除、导出、更新等功能，提供对 CA 证书管理的交叉认证功能。 系统应具备系统审计功能，提供对操作员的操作与登录的日志进行审计，输入审计的起始与结束时间，并输入需要审计的业务操作员名称或操作内容，可以查询到相关的操作日志，操作日志至少包括操作时间、操作员、操作名称、操作对象与操作结果等。 系统应能够对外提供标准的接口服务，供其它系统调用，以完成证书申请、证书发放和证书废止等业务操作并支持证书模板扩展信息配置功能。 系统应该具有基本系统配置功能，至少包括对服务参数、当前库、历史库、加密机、LDAP、 KM 服务和日志配置功能。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		系统应具有系统管理功能，能够提供管理根证书管理、证书模板管理、站点证书管理、身份证书管理、SPKM 证书管理、RA 的管理、日志管理、证书管理、系统维护、黑名单管理等功能。 系统应支持管理客户端可基于浏览器进行访问功能。 系统应提供数据迁移工具，保证新老平台数据一致性。 系统应支持 CA 用户证书的多种发布方式，发布模式至少包括 LDAP 模式、HTTP 模式等。 系统应支持自定义证书序列号长度、证书模板扩展信息自定义配置功能。 系统应具有优化权限管理功能，能够根据不同的管理角色赋予相对应权限。 双证书签发速度≥10 张/秒；数据库证书量≤10 万条时，多线程并发查询处理时间≤30ms；证书签发量为百万级。支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。			
2	KM 系统	核心架构换代，将原有 CS 架构换代为 BS 结构。 系统应同时支持国密算法和 RSA 算法。 系统应支持国产操作系统、数据库和服务器。 系统应至少具有服务配置、SPKM 配置、密钥生成和配置、加密机配置、密钥管理等系统管理配置功能。 系统应具有对 CA 密钥、用户密钥的全生命周期的管理，包括生产、存储、分发、销毁等。 系统应具有登录、数据库、当前库、历史库、日志、签名和密钥服务配置等功能。 系统具有统计功能并能够产生报表，至少应提供密钥使用情况、密钥分发\恢复\销毁情况的统计报表。 系统应支持 MOFN 方式保证司法取证安全，支持司法取证人员注册、查询和删除并提供密钥恢复功能。 在系统部署时设定的 M/N 值（N 个人中最少 M 个人到场）进行司法取证员的身份验证，需要选择每个司法取证人员证书进行签名，在 M 个司法取证人员的签名操作完成后，系统验证司法取证人员的合法性，验证通过后进行密钥恢复。 系统应提供数据迁移工具功能。 系统应支持报表管理，通过不同的查询方式，生成不同的报表。 系统应具有当前库和历史库配置功能，当前库存储在用密钥数据，历史库备份归档数据。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		支持对多个 CA 提供服务，可以通过对各个 CA 系统实施灵活的授权管理实现对各个 CA 系统服务的管理。双证书签发速度≥10 张/秒；数据库证书量≤10 万条时，多线程并发查询处理时间≤30ms；证书签发量为百万级。支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。			
3	RA 系统	核心架构换代，将原有 C/S 架构换代为 B/S 结构。 系统应同时支持国密 SM2 算法和 RSA 算法。 系统应支持国产操作系统、数据库和服务器。 系统应具有基于双算法的证书管理功能。如证书申请、更新、作废、审核、更新、注销、挂起、冻结、查询和下载签发等功能。 系统应具有用户信息管理功能，如查询用户、用户信息注册功能、用户信息批量注册功能、用户属性字典管理功能。 系统应具有机构管理功能，在系统中能够管理相应的机构信息并进行机构导入操作。 系统应具有业务数据的导入导出功能。 系统应具有根据介质号（UKEY 设备卡号）对用户证书进行查询统计功能，提供国密算法证书存储介质的管理功能。 系统应具有日志记录功能，能够详细记载证书签发行为，日志至少包括证书类型、签发时间、管理员等信息。 支持操作员权限的细分授权，支持批量注册、批量审核、批量签发和批量废除等批量化的操作功能。 用户管理、证书管理等功能单次请求处理时间＜0.3 秒；接收用户计算机发送的申请请求时，结合在线发证系统，签发证书的速度≥10 张/秒；支持 SM2 算法、RSA1024 和 RSA2048 算法；支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。	套	1	
4	AA 系统	系统架构为 B/S 架构且支持国密算法和 RSA 算法。 系统应提供 AA 证书模板管理，包括查询、更新、删除等功能。 系统应提供黑名单管理功能，能够下载 CRL 并对黑名单服务进行管理。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		系统应具有服务参数配置功能，提供当前库、历史库配置功能并支持 web 页面管理。 系统应具有加密机和日志配置功能。 系统应具有管理根证书管理、ARA 管理、系统维护、黑名单管理等。新增证书模板，更新证书模板，删除证书模板，ARA 站点增加、删除、查询等，系统备份，系统恢复。 系统应具有基本信息配置、当前库配置、加密机配置、日志配置等模块。 系统应支持多种证书类别认证。			
5	ARA 系统	系统架构为 B/S 架构且支持国密算法和 RSA 算法。 系统应具有个人属性管理、属性信息管理、证书审核管理、证书签发管理、证书拒绝管理，应用管理、应用属性管理、应用角色管理，机构管理、机构属性管理等，支持用户管理及数据同步。 系统应支持多种授权模式满足实际应用场景，如：用户授权、用户群组授权、机构授权以及属性授权等。支持应用接入，为接入应用分配接入凭证。管理应用的权限资源：包含角色、功能，以此为授权客体。 系统应具有职级属性注册、查询、更新、删除功能。 系统应具有个人属性证书注册、签发、更新审核等功能。支持警员、辅警等多种证书类别。 系统应该具有个人属性证书查询及显示详细信息功能，并支持警员等多证书信任域验证。	套	1	
6	证书综合审计查询系统	支持基于应用、用户（证书）、设备等维度综合日志审计。 支持对证书使用情况进行审计，可以对证书发放情况、运维情况、过期情况，要求支持按照地区、时间、状态、证书类型（包括普通数字证书和指纹数字证书、警员证书和辅警证书、移动警务数字证书、RSA 及 SM2 证书）等维度进行证书统计，要求能投提供统计数据及详细证书清单，并支持导出等功能。 能够接受或采集记录证书行为并审计数字证书的发证、制证、更新、注销、证书的使用等一系列证书行为状态和操作日志。 能够接受或采集指纹数字证书的发放、指纹证书的指纹录入、变更、删除等详细审计情况，并对频繁更换指纹等情况能够进行预警。 支持以用户（证书）角度进行日志审计，对用户访问统计、用户访问记录、详细用户查询、闲置用户查	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		询、活跃用户查询、在线用户查询。 支持集中认证网关设备实时访问行为的日志安全审计，包括日志信息的统一收集、集中管理和统计分析；接收、收集各类应用系统的操作日志、运行日志，实现违规事件、可疑行为的事后审计。 通过审计技术为系统管理员提供有价值的日志分析信息，从而帮助系统管理员及时发现系统入侵行为或潜在的系统漏洞，使系统管理员及时改进并加强安全防范措施;结合本省实际情况,证书审计系统管理员可查看所辖范围内警员和辅警证书应用访问记录和证书发放状态。 系统应支持千万级海量数据分析、统计，满足大用户应用系统的审计要求。			
7	集中运行监控与管理系统	系统应支持国密算法和 RSA 算法、国产操作系统、数据库和服务器。 支持警员证书、辅警证书等多种证书，支持警员、辅警证书信任域，支持证书行为趋势分析和应用的人员、网络边界分析。 支持全景监控功能。在首页上展现各被监控系统的拓扑图，并直观显示各设备是正常、故障、警告或是停止监控状态。在首页上展现各种监控状态的设备汇总数，以及最近一段时间的业务监控、网络监控、资源监控的汇总统计数据。 支持跨防火墙部署，系统通过数据推送代理工具，能够将监控消息发送至其它平台，达到监控效果。 支持性能分析功能，系统能够对多台硬件设备进行性能比较，并将比较结果进行直观展示。 支持重试探测，系统能够对单台监控设备设置重试次数和超时时间。 支持与第三方短信平台和电子邮件系统结合，可以将预警信息和故障信息推送到第三方产品进行的短信提醒。 系统应支持报表业务。	套	1	
8	警用数字证书一网通系统	系统应具有机构管理功能，管理功能至少包括查询、导入、批量导入、批量确认、删除、批量删除、批量确认、新增、修改、查看机构历史记录等功能，实现对机构的精准化管理。 系统应具有用户管理功能，管理功能至少包括人员批量导入、批量确认、批量删除、导入、修改、删除、确认、新增、注册、查询、冻结、解冻、人员修改用户解冻、查看人员历史记录、退休、返聘人员管理	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		等功能。 系统应支持在线的证书管理流程并提供数字证书查询、申请、制作、废除、更新、补发、延期、解锁、冻结、解冻、锁定、注销、证书补发申请、证书解冻申请、证书延期申请、属性变更、证书信息校验、已发证书管理等业务的线上流转，并能够 PKI 系统及字典管理相结合，简化证书制发流程，提高工作效率。 系统应具有介质编号管理功能，可对各地市介质进行统一管理。 系统应具有 license 管理、预警数据分析、审计管理、数据推送等功能。 系统应具有异常日志告警功能。 系统应具有证书统计报表功能，能够依据时间段对各单位的发证量、发证率、自定义发证量等信息进行统计并以报表形式展示。 系统支持操作审计查询功能，通过相应的查询条件可以至少查到某个证书的证书信息、申请状态、是否锁定、操作人、存储介质、客户端和操作时间等。支持特殊角色、PIN 码、证书管理员、审计管理员等管理。 支持与第三方短信平台对接，在自动申请证书时，可通过手机短信码或邮箱进行验证，也可将证书异常状态信息即时反馈给证书拥有者。 系统应具有证书管理功能，能够对证书和介质进行管理，证书管理应至少包括监管证书、证书待处理、证书的申请管理、已发证书管理、异常证书管理、站点证书管理、鉴别评估、证书统计报表等功能。 系统应具有证书自助更新功能,对于已签发的RSA的证书可以自助更新升级为支持国产密码算法的证书，实现平滑过渡。系统应具有个人行为轨迹、退休用户预警、异常时间段访问预警、人证不符预警、证书到期预警、证书活跃度预警、退休证书使用预警、异常时间段访问预警、异常 IP 地址预警等功能。 统一的证书管理门户，能够与警员、辅警 PKI 系统联动，提供统一的管理操作，实现业务的统一入口，简化管理员的操作并提供统一的证书服务。 系统应支持在线管制功能，当辅警或责任民警单位信息、身份证号等信息一旦变更，系统能够自动锁定			

序号	名　称	技术参数要求	单位	数量	备注
		证书，需要手动重新确定监管关系才能恢复使用。			
9	集中认证网关	集中认证网关实现与公安 PKI 基础设施（公安警员 PKI、辅警 PKI 系统）对接，实现用户基于数字证书的身份认证。安全认证网关作为应用中间件，基于 PKI 技术，将证书与业务系统进行关联，实现警员和辅警登录业务系统的强身份验证，同时基于数字证书的唯一特性，实现统一认证服务。 支持警员和辅警证书等多种证书类型的身份认证，对于公安未来定义的证书类型保持扩展设计，以便在新证书类型出现时能够无缝结合。 实现为多个业务系统提供身份鉴别服务，形成集中式的透明服务模式，并采用安全传输隧道完成终端与服务端之间数据的安全传输。 支持国密 SM1/SM2/SM3/SM4 算法，RSA1024 和 RSA2048 算法。 冗余电源，i7CPU（或至强），16Gb 内存，网络接口≥6 千兆口；最大并发连接数≥5500；最大并发用户数：≥4000 个；设备吞吐率：≥850Mbps；每秒完成交易数（TPS）：40000 次/秒； 最大新建连接数 RSA1024：10000 次/秒；最大新建连接数 RSA2048：3000 次/秒；最大新建连接数 SM2：4000 次/秒。 支持多条证书链同时存在、同时生效，即同一个 SSL 服务可以同时认证多家 CA 中心的证书用户。 多服务多应用证书支持：可以建立多个服务，保护不同的应用，每个应用或服务可以使用不同的证书及策略；客户端证书认证多样化策略支持：可以灵活配置建立认证用户证书的策略，包括强制认证，可选认证，仅信任本地证书链等；协议自适应适应支持：系统可以在同一个服务实例中，同时支持国际标准协议（TLS 1.0/1.1/1.2）以及国家密码管理局制定的国密 SSLVPN 协议。根据客户端的支持情况自动适应。 系统可以将用户证书信息包括扩展项信息传送给应用系统；认证一致性：系统通过特有的 HTTP 注入（Cookie/Header）技术将用户的证书信息传送给后台应用，使应用无需证书接口开发就可以方便的获取用户证书信息；自动登录功能：对于特定应用，系统采用用户映射技术，将证书映射为原有系统中的账户，并进行自动登录，在后台应用无需修改的情况下实现单点登录；策略统一下发：系统实现客户端	套	2	

序号	名　称	技术参数要求	单位	数量	备注
		策略的统一下发，用户无需对客户端进行任何配置；错误重定向：系统对于认证错误可以重定向到用户指定页面，增强友好性；访问控制功能：实现 URL 级别的访问控制，对于不同用户、不同角色实现不同的控制。 产品必须在国家密码管理局《支持 SM2/3/4 密码算法的商用密码产品目录》备案，提供高性能网关检测报告相关证明材料。			
10	密码机	支持国密 SM1/SM2/SM3/SM4 算法，RSA1024 和 RSA2048 算法；提供数字签名、验签接口。 SM1 算法（128 位）密钥加解密速率≥110Mbps；SM2 算法（256 位）签名速率≥700 次/秒，验签速率≥180 次/秒；SM3 运算速率≥150Mbps；RSA 算法（2048 位）签名速率≥850 次/秒，验签速率≥9500 次/秒；支持最大并发数≥500；平均故障间隔时间(MTBF)：>40000 小时。 采用物理噪声发生器，可以生成满足要求的真随机数；支持对称、非对称密钥的产生、存储和销毁，保证密钥在生存周期的各个环节的安全性；提供访问权限控制，密码机采用防拆、防撬结构设计，保证物理安全；提供实时监控系统的安全日志。 可以根据需要利用内部存储的 RSA/SM2 私钥或外部导入 RSA/SM2 私钥对请求数据进行数字签名，支持基于 RSA/SM2 密码算法的数字信封功能，并支持由内部密钥保护到外部密钥保护的数字信封转换功能，支持基于主密钥保护下的密钥的备份和恢复功能，保证了安全应用系统的安全性和可靠性。 数字签名的产生和验证：可以根据需要利用内部存储的 RSA/SM2 私钥或外部导入 RSA/SM2 私钥对请求数据进行数字签名。 密钥的安全存储：设备内可存储 50 对 RSA 密钥对（包括签名密钥对和加密密钥对）和 50 对 SM2 密钥对，并且私钥部分受系统保护密钥的加密保护。 提供访问权限控制，密码机防拆、防撬结构设计，保证物理安全。	套	4	
11	目录服务	支持主从结构，支持一主多从和多主多从的部署方式；主从配置时支持自动测试，可以清晰的知道从 LDAP 的存活状态。单服务管理容量可达千万级条目。 支持 SM2 算法数字证书、CRL 级目录服务地址等证书目录数据对外发布。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		支持 LDAP V2、V3 标准，支持标准的 LDIF 格式；支持 X509 V3 标准。 提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力。 与身份认证网关联动，供身份认证网关获取用户的属性证书；支持 RFC 规范定义的分页标准（RFC2696），用户可以分页异步读取数据，而无须一次获取全部。 最大并发连接数≥1000；在线精确查询时间（30 万级）：单线程响应时间＜1ms，50 线程响应时间＜20ms；在线模糊查询时间（30 万级）：单线程响应时间＜130ms，50 线程响应时间＜300ms；吞吐量 30 万条目≥2500 次/秒（50 线程精确查询）。			
12	警员 USB KEY	公安数字证书。 采用 USB 接口设计，标准 USB 1.1 设备，支持 USB2.0 接口。 基于公钥体系的数字证书和私钥的安全载体，保证数字证书和私钥的合法使用；支持 RSA、DES、3DES、SHA-1、SSF33、SM1、SM2 算法。需符合公安部统一要求。	套	3000	
（二）		辅警 PKI 系统建设			
1	辅警 CA 系统	系统应具有对 SM2 算法体系支持，包括 CA 签名证书密钥算法、用户证书密钥算法、服务器证书密钥算法、管理员证书密钥算法。 系统应支持基于双算法的证书申请、下载、更新、冻结、解冻、注销证书等功能。 系统应支持国产操作系统、数据库和服务器。 系统应支持归档证书的存储，确保归档证书信息的完整性和易用性。 系统应提供 CRL 服务，具有黑名单管理功能，可以同步 CRL 至 LDAP，黑名单发布模式应支持但不限于增量 CRL 和全量 CRL 的发布模式。 系统应支持 CA 策略管理功能，可以为 CA 证书制定不同的策略，配置策略应包括但不限于管理员证书的策略配置、个人 RSA/国产密码双证书的策略配置、设备证书的策略配置、域控制器证书的策略配置。各类型证书策略配置模板应包括但不限于证书有效期的配置和密钥用法的配置。 系统应具有 CA 证书管理的功能，主要包括查询、生成、导出、导入、取消和撤销功能并且应具有对下级 CA 进行签发、查询、废除、导出、更新等功能，提供对 CA 证书管理的交叉认证功能。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		系统应具备系统审计功能，提供对操作员的操作与登录的日志进行审计，输入审计的起始与结束时间，并输入需要审计的业务操作员名称或操作内容，可以查询到相关的操作日志，操作日志至少包括操作时间、操作员、操作名称、操作对象与操作结果等。 系统应能够对外提供标准的接口服务，供其它系统调用，以完成证书申请、证书发放和证书废止等业务操作并支持证书模板扩展信息配置功能。 系统应该具有基本系统配置功能，至少包括对服务参数、当前库、历史库、加密机、LDAP、 KM 服务和日志配置功能。 系统应具有系统管理功能，能够提供管理根证书管理、证书模板管理、站点证书管理、身份证书管理、SPKM 证书管理、RA 的管理、日志管理、证书管理、系统维护、黑名单管理等功能。 系统应支持管理客户端可基于浏览器进行访问功能。 系统应支持 CA 用户证书的多种发布方式，发布模式至少包括 LDAP 模式、HTTP 模式等。 系统应支持自定义证书序列号长度、证书模板扩展信息自定义配置功能。 系统应具有优化权限管理功能，能够根据不同的管理角色赋予相对应权限。 双证书签发速度≥10 张/秒；数据库证书量≤10 万条时，多线程并发查询处理时间≤30ms；证书签发量为百万级。支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。			
2	辅警 KMC 系统	系统应同时支持国密算法和 RSA 算法。 系统应支持国产操作系统、数据库和服务器。 系统应至少具有服务配置、SPKM 配置、密钥生成和配置、加密机配置、密钥管理等系统管理配置功能。 系统应具有对 CA 密钥、用户密钥的全生命周期的管理，包括生产、存储、分发、销毁等。 系统应具有登录、数据库、当前库、历史库、日志、签名和密钥服务配置等功能。 系统具有统计功能并能够产生报表，至少应提供密钥使用情况、密钥分发\恢复\销毁情况的统计报表。 系统应支持 MOFN 方式保证司法取证安全，支持司法取证人员注册、查询和删除并提供密钥恢复功能。 在系统部署时设定的 M/N 值（N 个人中最少 M 个人到场）进行司法取证员的身份验证，需要选择每个司	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		法取证人员证书进行签名，在 M 个司法取证人员的签名操作完成后，系统验证司法取证人员的合法性，验证通过后进行密钥恢复。 系统应提供数据迁移工具功能。 系统应支持报表管理，通过不同的查询方式，生成不同的报表。 系统应具有当前库和历史库配置功能，当前库存储在用密钥数据，历史库备份归档数据。 支持对多个 CA 提供服务，可以通过对各个 CA 系统实施灵活的授权管理实现对各个 CA 系统服务的管理。 双证书签发速度≥10 张/秒；数据库证书量≤10 万条时，多线程并发查询处理时间≤30ms；证书签发量为百万级。支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。			
3	辅警 PKI 目录	支持主从结构，支持一主多从和多主多从的部署方式；主从配置时支持自动测试，可以清晰的知道从 LDAP 的存活状态。单服务管理容量可达千万级条目。 支持 SM2 算法数字证书、CRL 级目录服务地址等证书目录数据对外发布。 支持 LDAP V2、V3 标准，支持标准的 LDIF 格式；支持 X509 V3 标准。 提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力。 与身份认证网关联动，供身份认证网关获取用户的属性证书；支持 RFC 规范定义的分页标准（RFC2696），用户可以分页异步读取数据，而无须一次获取全部。 最大并发连接数≥1000；在线精确查询时间（30 万级）：单线程响应时间＜1ms，50 线程响应时间＜20ms；在线模糊查询时间（30 万级）：单线程响应时间＜130ms，50 线程响应时间＜300ms；吞吐量 30 万条目≥2500 次/秒（50 线程精确查询）。	套	1	
4	辅警 PKI 地址目录	通过辅警中央地址目录复制全国辅警目录服务查询路径，完成目录树的引用查询。 支持主从结构，支持一主多从和多主多从的部署方式；主从配置时支持自动测试，可以清晰的知道从 LDAP 的存活状态。单服务管理容量可达千万级条目。 支持 SM2 算法数字证书、CRL 级目录服务地址等证书目录数据对外发布。 支持 LDAP V2、V3 标准，支持标准的 LDIF 格式；支持 X509 V3 标准。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力。 与身份认证网关联动，供身份认证网关获取用户的属性证书；支持 RFC 规范定义的分页标准（RFC2696），用户可以分页异步读取数据，而无须一次获取全部。 最大并发连接数≥1000；在线精确查询时间（30 万级）：单线程响应时间＜1ms，50 线程响应时间＜20ms；在线模糊查询时间（30 万级）：单线程响应时间＜130ms，50 线程响应时间＜300ms；吞吐量 30 万条目≥2500 次/秒（50 线程精确查询）。			
5	辅警 USB KEY	公安辅警数字证书介质。 提供数字证书存储，支持国密及 RSA 双算法。 采用 USB 接口设计，标准 USB 1.1 设备，支持 USB2.0 接口。 基于公钥体系的数字证书和私钥的安全载体，保证数字证书和私钥的合法使用；支持 RSA、DES、3DES、SHA-1、SSF33、SM1、SM2 算法。需符合公安部统一要求。	套	1000	
（三）		移动警务 PKI 系统建设			
1	CA	系统应具有对 SM2 算法体系支持，包括 CA 签名证书密钥算法、用户证书密钥算法、服务器证书密钥算法、管理员证书密钥算法。 系统应支持基于双算法的证书申请、下载、更新、冻结、解冻、注销证书等功能。 系统应支持国产操作系统、数据库和服务器。 系统应支持归档证书的存储，确保归档证书信息的完整性和易用性。 系统应提供 CRL 服务，具有黑名单管理功能，可以同步 CRL 至 LDAP，黑名单发布模式应支持但不限于增量 CRL 和全量 CRL 的发布模式。 系统应支持 CA 策略管理功能，可以为 CA 证书制定不同的策略，配置策略应包括但不限于管理员证书的策略配置、个人 RSA/国产密码双证书的策略配置、设备证书的策略配置、域控制器证书的策略配置。各类型证书策略配置模板应包括但不限于证书有效期的配置和密钥用法的配置。 系统应具有 CA 证书管理的功能，主要包括查询、生成、导出、导入、取消和撤销功能并且应具有对下	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		级 CA 进行签发、查询、废除、导出、更新等功能，提供对 CA 证书管理的交叉认证功能。 系统应具备系统审计功能，提供对操作员的操作与登录的日志进行审计，输入审计的起始与结束时间，并输入需要审计的业务操作员名称或操作内容，可以查询到相关的操作日志，操作日志至少包括操作时间、操作员、操作名称、操作对象与操作结果等。 系统应能够对外提供标准的接口服务，供其它系统调用，以完成证书申请、证书发放和证书废止等业务操作并支持证书模板扩展信息配置功能。 系统应该具有基本系统配置功能，至少包括对服务参数、当前库、历史库、加密机、LDAP、 KM 服务和日志配置功能。 系统应具有系统管理功能，能够提供管理根证书管理、证书模板管理、站点证书管理、身份证书管理、SPKM 证书管理、RA 的管理、日志管理、证书管理、系统维护、黑名单管理等功能。 系统应支持管理客户端可基于浏览器进行访问功能。 系统应支持 CA 用户证书的多种发布方式，发布模式至少包括 LDAP 模式、HTTP 模式等。 系统应支持自定义证书序列号长度、证书模板扩展信息自定义配置功能。 系统应具有优化权限管理功能，能够根据不同的管理角色赋予相对应权限。 双证书签发速度≥10 张/秒；数据库证书量≤10 万条时，多线程并发查询处理时间≤30ms；证书签发量为百万级。支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。			
2	RA	系统应同时支持国密 SM2 算法和 RSA 算法。 系统应支持国产操作系统、数据库和服务器。 系统应具有基于双算法的证书管理功能。如证书申请、更新、作废、审核、更新、注销、挂起、冻结、查询和下载签发等功能。 系统应具有用户信息管理功能，如查询用户、用户信息注册功能、用户信息批量注册功能、用户属性字典管理功能。 系统应具有机构管理功能，在系统中能够管理相应的机构信息并进行机构导入操作。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		系统应具有业务数据的导入导出功能。 系统应具有根据介质号（UKEY 设备卡号）对用户证书进行查询统计功能，提供国密算法证书存储介质的管理功能。 系统应具有日志记录功能，能够详细记载证书签发行为，日志至少包括证书类型、签发时间、管理员等信息。 支持操作员权限的细分授权，支持批量注册、批量审核、批量签发和批量废除等批量化的操作功能。 用户管理、证书管理等功能单次请求处理时间＜0.3 秒；接收用户计算机发送的申请请求时，结合在线发证系统，签发证书的速度≥10 张/秒；支持 SM2 算法、RSA1024 和 RSA2048 算法；支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。			
3	KMC	系统应同时支持国密算法和 RSA 算法。 系统应支持国产操作系统、数据库和服务器。 系统应至少具有服务配置、SPKM 配置、密钥生成和配置、加密机配置、密钥管理等系统管理配置功能。 系统应具有对 CA 密钥、用户密钥的全生命周期的管理，包括生产、存储、分发、销毁等。 系统应具有登录、数据库、当前库、历史库、日志、签名和密钥服务配置等功能。 系统具有统计功能并能够产生报表，至少应提供密钥使用情况、密钥分发\恢复\销毁情况的统计报表。 系统应支持 MOFN 方式保证司法取证安全，支持司法取证人员注册、查询和删除并提供密钥恢复功能。 在系统部署时设定的 M/N 值（N 个人中最少 M 个人到场）进行司法取证员的身份验证，需要选择每个司法取证人员证书进行签名，在 M 个司法取证人员的签名操作完成后，系统验证司法取证人员的合法性，验证通过后进行密钥恢复。 系统应提供数据迁移工具功能。 系统应支持报表管理，通过不同的查询方式，生成不同的报表。 系统应具有当前库和历史库配置功能，当前库存储在用密钥数据，历史库备份归档数据。 支持对多个 CA 提供服务，可以通过对各个 CA 系统实施灵活的授权管理实现对各个 CA 系统服务的管理。	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		双证书签发速度≥10 张/秒；数据库证书量≤10 万条时，多线程并发查询处理时间≤30ms；证书签发量为百万级。支持多种大型数据库系统和目录服务系统，包括 Oracle、MSsql、mysql 等。			
4	目录服务	支持主从结构，支持一主多从和多主多从的部署方式；主从配置时支持自动测试，可以清晰的知道从 LDAP 的存活状态。单服务管理容量可达千万级条目。 支持 SM2 算法数字证书、CRL 级目录服务地址等证书目录数据对外发布。 支持 LDAP V2、V3 标准，支持标准的 LDIF 格式；支持 X509 V3 标准。 提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力。 与身份认证网关联动，供身份认证网关获取用户的属性证书；支持 RFC 规范定义的分页标准（RFC2696），用户可以分页异步读取数据，而无须一次获取全部。 最大并发连接数≥1000；在线精确查询时间（30 万级）：单线程响应时间＜1ms，50 线程响应时间＜20ms；在线模糊查询时间（30 万级）：单线程响应时间＜130ms，50 线程响应时间＜300ms；吞吐量 30 万条目≥2500 次/秒（50 线程精确查询）。	套	1	
5	移动身份认证网关	支持国密 SM1/SM2/SM3/SM4 算法，RSA1024 和 RSA2048 算法。 冗余电源，i5CPU（或至强），8Gb 内存以上，网络接口≥6 千兆口；最大并发连接数≥5500；设备吞吐率：≥850Mbps；每秒完成交易数（TPS）：30000 次/秒。 支持 TLS 1.0/1.1/1.2 和国密 SSLVPN 多协议栈。 支持管理员三权分立功能。 支持接入控制，只符合条件的终端类型才可接入。 支持访问控制，只允许角色访问特定的资源。 支持与多种外部系统进行联动（包括鉴别评估与管理系统等权限系统）。 服务热备：网关支持双机热备，实现服务连续性和无缝切换，切换时间<2 秒。 自恢复机制：在系统发生异常失去响应情况下可以自行硬件重启动，恢复服务。 完善的监控、报警机制：对系统的关键资源和指标进行图形化监控，对于异常情况可以进行报警，有利	台	2	

序号	名　称	技术参数要求	单位	数量	备注
		于提前发现并解决问题。 快速恢复：在服务端服务异常重启后，可通知客户端重新建立连接，客户端快速同步服务端同步状态，保证业务的流畅进行。			
6	移动签名服务器	冗余电源，i5 CPU（或至强），8Gb 内存以上，网络接口≥6 千兆口；最大并发连接数≥5500；最大并发用户数：≥4000 个；设备吞吐率：≥850Mbps；RSA(1024 位)签名：5000 次/秒；RSA(1024 位)验签：8000 次/秒；RSA(2048 位)签名：4500 次/秒；RSA(2048 位)验签：7000 次/秒；SM2(256 位)签名：3000 次/秒；SM2(256 位)验签：1500 次/秒。 支持提供普通格式，PKCS#7 Attach/Detach 等多种格式的数字签名功能。 支持提供普通格式，PKCS#7 Attach/Detach 等多种格式的数字签名验证功能。 支持提供证书解析功能，获取证书中的任意主题信息以及扩展项信息。 支持根据不同的签名证书创建多个服务实例，由调用者选择使用。 文件签名功能：对文件提供数字签名功能（在 API 中计算摘要） 文件验证签名功能：对文件提供数字签名验证功能（在 API 中计算摘要） 数字信封功能：提供 PKCS#7 格式的数字信封加密和解密功能。 支持商用密码算法 SM2/SM3/SM4，支持国际通用算法 RSA/AES/SHA1 等。 支持原文数据签名、文件签名、哈希后签名及 PKCS＃7 等格式签名数据的验证。 产品部署模式应支持串联部署，并联部署、热备部署和自负载部署模式。	台	4	
7	移动身份认证组件/移动数字签名组件/移动	移动警务终端上的移动身份认证组件 APP，支持 SM2 和 RSA 算法。 支持在国家密码管理局备案的各种类型的终端密码模块，包括 TF 卡、软介质、移动终端自带安全芯片等。 支持连接移动身份认证网关访问移动警务公安信息网，实现基于用户证书的身份认证。 实现基于国密 SM2 算法的传输数据签名验签、传输数据加密解密、终端数据加密存储。	台	1	

序号	名　称	技术参数要求	单位	数量	备注
	加密组件	支持 VPN 隧道。支持对常见的 UDP 应用和 TCP 应用全面保护，包括身份和链路加密，通信数据实现加密传输。			
8	警用数字证书一网通系统空中发证模块	实现移动警务证书全生命周期管理，包括在线签发、申请、延期、废除、审核，提供快捷、安全的移动警务证书制发体系。 通过移动证书管理组件实现采集用户终端信息、发起证书操作请求、解析证书操作响应和调用密码模块实现移动警务证书的各项管理功能。 能够实现发证管控，防止频繁发起的恶意和非法证书请求。 使用安全的套接字协议，直接对接 RA 实现安全发证。 根据密钥使用的非对称算法类型来区分，支持签发 RSA 证书、SM2 证书。 根据证书类型（数量）来区分，支持签发双证书（RSA、SM2）、单证书（RSA、SM2）。 根据密钥位数来区分，支持签发 1024、2048 位的 RSA 证书、SM2 证书。 个人凭据（数字证书、私钥）需支持接入多种类型（厂商）的存储介质，以满足不同的安全要求级别。 支持证书签发到加密的软件区域、硬件 TF 区域等。	台	1	
9	空中发证身份校验网关	具备 inSE 密码模块授权动态控制功能，支持基于设备信息的 inSE 密码模块注册授权。 支持 inSE 密码模块的在线管理、统计和历史记录查询功能。 支持人像活体采集信息校验功能。 支持多种人像认证模式：单人像（身份信息+人像采集信息）、双人像（人像采集信息+标准人像信息）。 支持多标准人像信息源（人口库、本地库、自有库等）比对和信息源定制功能（可根据用户需求定制标准人像信息源）。 具备认证信息统计、查询和管理功能，支持本地人像信息留存建库功能。 支持基于终端信息的终端认证功能。 支持根据用户策略，设定多种认证方式组合认证功能； 支持用户手动选择认证机制。	台	1	

序号	名　称	技术参数要求	单位	数量	备注
		基于 B/S 结构的管理界面，可支持 HTTPS 安全远程管理； 具备操作审计功能；具备异常发现和告警功能。 最大并发连接数：≥500；密码模块授权速率：≤100ms；人像比对速率：≤300ms；人像识别率：≥98%（错误接受率≤0.01%）；身份证校验速率：≤500ms；设备认证速率：≤100ms。			
10	警用移动数字证书自助服务系统	移动警务空中发证前置服务 。 支持直接向安卓 5.0 以上手机端签发证书。 支持 RSA、SM2 双算法。 提供 PKICS11、CSP、SKF 和其他扩展接口，提供 XML、JSON、HTTP、HTTPS 通讯协议。通信数据的加密采用 HTTPS 实现，提供介质类型管理服务。 系统提供数字证书申请、更新、延期、冻结、注销业务等证书在线服务。	套	1	
11	警用移动终端数字证书管理系统	移动警务空中发证客户端 APP。 终端密码安全模块实现证书和密钥对的安全存储和使用。用户可以进行证书查看、证书更新、证书延期、证书废弃等操作。 客户端支持对外服务接口，方便第三方应用系统调用证书密码服务，集成基于国密证书的安全存储、管理及短信验证、服务配置、系统重置等模块。 具备终端内用户证书的管理功能，可无缝对接空中发证服务，实现用户自助证书管理，包括证书自助申请、证书自助更新、证书自助下载、证书自助延期、证书自助注销等功能。 安全通道身份鉴别和密钥交互满足国密标准，即规范《0024-2014_SSLVPN 技术规范》。 个人凭据（数字证书、私钥）的存储介质接口符合国密标准，即《0016-2012_智能 IC 卡及智能密码钥匙密码应用接口规范》。	套	1	
（四）	服务器以及网络设备				

序号	名　称	技术参数要求	单位	数量	备注
1	PKI 系统服务器	机架式服务器，服务器高度≥2U，标配原厂导轨。 CPU: ≥2 颗 Intel SP 4110，单颗核芯≥10 核,双线程，主频≥2.1GHz。 内存：≥32G DDR4 内存，频率≥2400MT，可扩展≥24 个内存插槽，最大支持最大容量 3.0TB。 硬盘：≥8 个 2.5 寸热插拔硬盘槽位，≥ 3*300G 10K SAS，可扩展至≥40 个热插拔硬盘槽位，提供官网截图并加盖生产厂商项目授权章。 网卡：≥4*GE 电口。 HBA 卡：≥1 块双通道 8Gb FC HBA 卡。 DVD：≥1 个 DVD-RW 光驱。 RAID 卡：≥1 个板载 专用插槽的 Raid 阵列卡，支持 Raid0/1/10/5，≥1GB 缓存，含断电保护。 最多提供≥10 个 PCIE3.0 插槽（其中可支持≥3 个全宽高性能 GPU 卡），提供官网截图并加盖生产厂商项目授权章。 电源：本次配置 2 个≥500w 热插拔冗余电源，1+1 冗余电源。 配置≥1Gb 的远程管理控制端口，配置虚拟 KVM 功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新 Firmware、虚拟媒体等操作，提供服务器健康日记、故障现场还原，支持智能电源管理，支持服务器内部温度切面的 3D 显示，可支持动态功率封顶。 产品生产厂商应具有健全的环保体系，建立有害物质的检测手段，严格管理产品采购和生产环节，禁止或控制有毒有害物质的使用。需通过 QC 080000 有害物质过程管理体系认证，提供证书复印件，并加盖原厂商公章或投标专用章。 为保证本项目的完善实施、严格按照要求落地，制造厂商均须具备良好的商业信誉，提供国家企业信用信息公示系统（网址：http://www.gsxt.gov.cn/）上行政处罚信息一栏的网站截图（带完整 URL 链接）证明，在“行政处罚内容“栏目内无行政处罚记录，并加盖厂商项目授权章。	台	16	
2	交换机	固化千兆以太网电接口≥24，上行千兆光接口数量≥4。 交换容量 ≥ 330 Gbps，包转发率≥90Mpps。	台	4	

序号	名　称	技术参数要求	单位	数量	备注
		MAC 地址表项≥16K，路由表项≥512。 支持 IPv4 静态路由、RIP V1/V2、OSPF。 支持基于端口的 VLAN、基于 MAC 的 VLAN。 支持基于协议 VLAN。 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms。 支持 DHCP Snooping，防止欺骗的 DHCP 服务器。 支持 ARP 检测来抵御 ARP 欺骗攻击。 支持 IPv6 地址。 为响应国家低碳的要求，产品厂商在产品设计、研发、生产、过程需采取有效减少温室气体排放措施，符合国家温室气体排放和清除的量化和报告的规范。产品生产厂商需通过 ISO 14064 温室气体核查，需提供报告复印件和国家认证认可监督管理委员会官网截图并加盖设备厂商公章。			
3	防火墙	采用非 X86 多核架构，机架规格为 1U；冗余双电源。 ≥16 个千兆电接口，8 个千兆光口；2 个 USB 接口，1 个 RJ45 串口。 支持 2 个扩展插槽。 最大并发连接数 100 万，每秒新建连接数 3 万。 支持透明、路由、混合及单臂等多种部署模式。 支持双机热备功能，支持高可靠性（包含主备/主主模式）部署，上述功能要求须提国家相关部委认可的第三方实验室测试报告证明。 支持静态路由、RIP 及 OSPF 动态路由、支持应用的策略路由。 支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。需提供设备功能界面截图证明，并加盖原厂项目授权章。 支持访问控制，会话控制等功能，流量控制。	台	3	

序号	名　称	技术参数要求	单位	数量	备注
		实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。 实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。 支持 IPV6。 为保证投标产品厂商在安全漏洞方面的整体研究水平和及时预防能力。具备网络安全漏洞统一收集验证、预警发布及应急处置体系，进而提高产品的安全性。产品生产厂商须成为国家信息安全漏洞共享平台（CNNVD）一级技术支撑单位和中国国家信息安全漏洞库（CNVD）技术组成员(提供相应证明材料并加盖生产厂商项目授权章)，提供证明材料并加盖生产厂商项目授权章。 投标产品供应商需具备科学、系统的知识产权管理体系。能够全面保护、并系统管理知识产权，支撑企业的技术创新能力。通过知识产权管理体系认证，要求提供证书复印件并加盖设备厂商公章。			
	五、应用支撑平台				
1	统一民生服务开放平台	流程模板库 页面模板库 业务组件库 基础组件库 视觉设计 UI 库 标准 SDK 开放能力 分项目控制台 服务中心 服务中心控制台	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		管理控制台 分项目控制台			
2	统一跨网数据交换平台	应用网关 API 网关 服务认证 日志监控 业务应用接入支持服务	套	1	
3	统一民生警务运营平台	数据采集 数据分析 数据运营 运营管理	套	1	
4	统一移动管理支撑平台	统一用户管理 统一授权管理 统一鉴权管理 移动应用管理 应用门户 移动应用评价 移动应用部署 开发商管理 开发资源管理 开发规范	套	1	
5	统一公安可信认证	公安可信身份认证 ″主要实现公安内部及外部的实名核身认证服务能力，同时可以将实名核身数据采集到公安内部。包括如下功能：	套	1	

序号	名　称	技术参数要求	单位	数量	备注
	平台	实名核身认证网关：实名认证、实名实人认证、路由调度、鉴权服务、负载均衡、数据传输安全； 移动端 SDK：提供移动端应用的实名核身 SDK 包； 融合比对服务：包括人脸比对引擎、活体检测引擎，采用本地自建模式，数据（图像、视频）落地公安网； 业务系统接入申请和管控：包括业务系统接入管理、业务系统接入申请、业务系统监控； 实名核身数据库：包括身份摘要信息库、人像比对特征库、审计日志、视频信息、人像信息等数据存储管理； 外部认证源对接：包括公安部一所互联网+身份认证平台； 跨网支撑：支持在公安一类区、二类区的实名核身服务，满足公安内外部的实名认证支持。 业务接入支撑：配合业务系统接入公安可信认证平台的实施技术支撑工作； 〞			
6	统一智能客服平台	智能客服系统 知识库机器人 多层级语料库管理 语音识别 知识库整理 知识库标注 界面个性化定制	套	1	
7	互联网中间件服务能力集成	集成统一申办受理平台 集成统一支付平台 集成统一物流平台 集成电子印章 集成电子证照服务	套	1	

序号	名　称	技术参数要求	单位	数量	备注
		集成互联网地图服务 集成政府授权的第三方服务 集成政府业务系统开放能力			
8	私有化中间件服务建设	OCR 服务、位置服务、短信服务平台、通用 mPaaS、通用应用开发框架、分布式关系型数据库、WEB 中间件、NoSQL 数据库、微服务框架、微服务熔断保护子系统、容器服务、工作流引擎服务	套	1	
9	统一运维管理平台	工单 设备管理 业务管理 统一监控 用户及权限管理 持续部署 标准化发布管理 数据备份与恢复	套	1	
10	系统软件及其他工具软件	操作系统 Windows 2012 Server 标准版 操作系统 CentOS　7.0 64 位或以上版本 数据库 Mongo 数据库 4 数据库 MySql 数据库 5.7 数据库 Redis 数据库 3.2+	套	1	
	六、安全保障体系				
1	安全服务		套	1	

4.2 海南公安“智慧微警务”项目软件开发

序号	名 称	技术参数要求	单位	数量	备注
（一）	便民惠企应用	1、户政（治安）业务功能：包括户口申报、户口迁入、户口迁出、市县内迁移、户口注销、立分户、证件办理、便民查询等功能。 2、治安业务功能：包括娱乐场所登记备案、管制器具备案、危险化学品备案、民用爆炸品备案等相关业务功能。 3、交管业务功能：包括驾驶证业务、交通违法处理、机动车业务、预选车牌、考试预约、事故快处、通行证办理移机交通违法异议申诉受理等业务功能。 4、出入境业务功能：包括证照网约先办、便民服务查询、线上业务办结、线下服务预约、综合业务办理、企业服务预约以及政务信息公开等业务功能。 5、综合警种业务功能：包括监管、宣传、禁毒、网安等警种业务的在线办理和操作指南等业务功能。	套	1	
（二）	利警应用	即时通讯（警务微信）：似于“微信”的即时通信工具，主要解决省厅内部的即时沟通、移动办公、一体化集成化办公的问题。 日常应用：构建沟通，协同，社交于一体的海南省公安智慧微警务平台，包括：移动 OA、动态（朋友圈）、厅长点评推送、通知公告、会议助手、新闻推送、业务看板、维修报障、督办、要情速递等 10 个应用。 专业应用：包括云搜、云回答、社区警务、党建、情报、指挥等警务应用。	套	1	

5 项目相关要求

1、投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。

2、报价人要保持同采购人的密切联系，遇有重大事项及时报告和反馈信息，尊重项目业主方的意见，接受项目业主方的提议、监督和指导。

3、投标人必须如实地对招标文件中各项技术要求作出明确的逐项响应承诺，并对其真实性负责。

4、投标人不得低于成本价恶意报价，若中标人报价过低（低于预算金额的80%），采购人有权要求中标人提供其报价与项目预算金额的差额作为履约保证金，同时预付款比例调整为 0，若中标人在实施过程中推诿扯皮，不按工期完成项目，采购人有权终止合同，没收履约保证金，并报主管部门严肃处理。

5、投标人应提交项目实施承诺函，否则投标文件将被拒绝。项目实施承诺函如下：

项目实施承诺函

致海南省公安厅：

如果我们投标文件被接受，我们将严格履行招标文件中规定的每一项要求及下述各项承诺，按期、保质保量履行合同的义务。

经贵方认可的工程项目负责人及相应资质的专业技术、管理人员是将来施工的现场的实际操作者，并常驻工程施工现场，上述人员未经招标人同意，我将不得擅自调换或撤离，若招标人认为有必要，可要求对上述人员的部分作出更好的调整，我方保证接收，全力配招标方打造精品工程。

针对招标文件中的“应用系统对接”部分工作。如我方中标 项目，我方将建立协调机制，保证现场对接有序、高效进行，提高工作效率。根据公司的相关规定，结合现场施工的的实际情况，及时修定协调程序。现场项目经理及管理人员根据协调程序的规定，积极与业主方、监理方等单位协调、沟通，确保工程顺利完成。在对接产生的工作量及相关协调成本及需要的网络设备，均已经包括在项目投标对应报价中，在项目实施过程将不对该部分产生增项费用。

应用系统对接需求如下：

“2.4 应用系统对接

2.4.1 便民惠企应用方面

2.4.1.1 与海南省一体化在线政务服务平台对接

实现与海南省一体化在线政务服务平台对接，主要对接如下：

（一）海南公安便民惠企服务应用能够按照省一体化在线政务服务平台的标准要求，与一体化在线政务服务平台入口（移动端和 PC 端）的对接，实现公安便民惠企服务在一体化在线政务服务平台中办理；

（二）海南公安梳理的便民惠企服务事项清单，根据省一体化在线政务服务平台的要求进行对接，实现公安服务事项清单同步到省政务服务清单中；

（三）海南公安采集的便民惠企的数据按照标准，实时提供给省政务服务平台及省其他厅直单位调用；

（四）便民惠企的数据进入公安网后，汇聚到公安信息资源服务平台，按照和省政府信息资源服务平台数据对接标准，定时按需把数据共享到省政府信息资源服务平台，为民众办理其他民生事项提供数据共享服务。

2.4.1.2 与公安部互联网+政务服务平台对接

实现与公安部互联网+政务服务平台对接，主要对接如下：

（一）海南公安便民惠企服务应用能够按照公安部的标准要求，与公安部互联网+政务服务平台对接，实现公安便民惠企服务在公安部互联网+政务服务平台中办理；

（二）海南公安梳理的便民惠企服务事项清单，根据公安部互联网+政务服务平台的要求进行对接，实现公安服务事项清单同步到公安部政务服务清单中；

（三）实现公安部用户平台在海南省微警务平台用户认证，部级平台登录后可以直接在省级平台办理业务；

（四）实现海南省级民生业务数据上报到公安部。

2.4.1.3 与海南省政府网站集约化平台对接

在咨询建议业务系统中，需要把社会公众提交的咨询和建议业务与海南省政府网站集约化平台对接，web 端提交的建议会进行筛选主动推送到政务云服务器上（可以匹配政务云上的身份证），管理员的回复都会主动的推送给服务器上。

2.4.2 利警服务应用方面

平台能够支持与现有移动警务应用对接，各业务警种根据业务需求，根据警务微信平台的统一接口规范标准，对现有的移动警务应用进行移动化改造，满足平台对接要求。”

承诺自承诺函签署日期开始在本项目建设过程中以及建设完成竣工移交日前持续有效。

承诺单位（盖章）：

法定代表人（职务、姓名）（签字并盖章）：

承诺日期：

B包采购需求

海南公安“智慧微警务”项目—警务流量（B包）

招标需求书

一、项目背景

为适应我省公安移动警务工作体系发展，移动警务业务量的增加，移动警务专网流量使用量增长，需为海南省公安厅机关民警购置警务流量服务。

二、用户需求

为海南省公安厅机关民警购置为期2年的警务流量服务。

三、技术需求

1、流量套餐需求：

提供700张手机通信卡，4G服务流量：包括不限量（超过40G后不额外计费）、不降速。

根据民警工作的实际需求，需要与各方进行沟通交流，比如办案调查，跨区域联合办案，提供便民服务等，移动警务终端通讯服务包含以下内容：

（1）SIM/UIM卡

（2）4G服务流量：包括不限量（超过40G后不额外计费）、不降速。运营商需提供必要的网络安全隔离措施，建立公安虚拟专用网络（如虚拟拨号专用网络 APN/VPDN），减少公安信息被泄漏、窃取和篡改的安全风险；采用必要的防范措施，防止对移动警务接入及应用系统的攻击；对网络安全事件的调查、发现和解决进行积极配合，并提供相关保障措施和承诺。

2、增值服务需求：

参照市面运营商话费套餐模式，配送700台移动警务专用终端。

（1）移动终端技术参数要求：

★警务安全双系统移动终端是一款保护公安警务工作秘密和敏感信息的智能移动终端设备，须通过公安部安全与警用电子产品质量检测中心GA/T 1466.1-2018和GA/T 1466.2-2018相关标准检测，具备双系统移动终端，完成移动警务的业务和功能。

1、杜绝后门:优先选用具备国产化核心部件、国产化操作系统、符合我国可信计算设计的安全移动操作系统，提供操作系统级的安全防护，完全杜绝android 等国外操作系统的后门隐患，防止移动终端信息泄露和移动终端被控。（提供工信部颁发的入网许可证明材料，并提供国产终端操作系统产品软件著作权证明）

2、闭环安全体系:目前最为完善的系统化安全设计，采用先进的闭环安全架构，提供从硬件到软件、从操作系统层到应用层、从端到云的闭环安全体系。全面实现防 root、防刷机、防泄漏、防破解的五防安全目标，具备强制访问控制、安全漏洞远程修复、存储数据加密等安全功能，与安全相关的核心代码必须自主可控。（提供公安部检测报告证明材料复印件）

3、双系统模式支持一机多能:两个系统之间秒级切换。双模式可分别接入互联网、公安信息网和指挥调度网，在充分保证公安信息网数据安全的基础上，将移动办公终端与个人通信终端合二为一，兼容安卓系统软件，解决了工作和生活交叉应用带来的信息安全风险，满足生活和工作的不同需求。（提供公安部检测报告证明材料复印件）

4、适用于业务和用户安全分级管理:基于安全双系统可接入不同的网络，可将不同安全等级的业务部署到不同的网络中：高安全性业务部署在公安信息网；基于公网的业务可部署到互联网。同一部警务专用移动终端可以接入多种网络，访问所有的业务，顺应公安信息化移动互联发展的趋势。也可以根据用户的不同，对访问的模式和业务进行限制。（提供公安部检测报告证明材料复印件）

★5、加密卡:可支持接入现有海南省公安厅移动警务平台（提供贴膜加密卡或者普通 TF 加密卡）。

（2）机型配置技术参数：

为满足民警日常工作需要，专用移动警务终端应满足以下参数：

主体	
外观设计	直板
操作系统	支持 Android 8.0 及以上版本
CPU 核数	八核
双卡	双卡双待单通

网络制式：支持移动/联通/电信 4G+/4G/3G/2G	
主卡	移动 4G（TD-LTE）/联通 4G（TD-LTE/LTE FDD）/电信 4G（TD-LTE/LTE FDD） 移动 3G（TD-SCDMA）/联通 3G（WCDMA）/电信 3G（CDMA 2000） 移动 2G（GSM）/联通 2G（GSM）/电信 2G（CDMA 1X）
副卡	移动 4G（TD-LTE）/联通 4G（TD-LTE/LTE FDD）/电信 4G（TD-LTE/LTE FDD） 联通 3G（WCDMA） 移动 2G（GSM）/联通 2G（GSM）/电信 2G（CDMA 1X）
屏幕	
屏幕尺寸	≥6.0 英寸
屏幕色彩	≥1670 万色
屏幕类型	OLED
▲分辨率	≥2244*1080 像素
触摸屏	多点触控触摸屏
传感器	
重力传感器	支持
环境光传感器	支持
接近光传感器	支持
霍尔传感器	支持
Camera 激光对焦传感器	支持
红外传感器	支持
色温传感器	支持
陀螺仪	支持
NFC	支持
指南针	支持
气压计	支持
存储	

▲运行内存(RAM)	≥6GB
▲机身内存(ROM)	≥128GB
最大支持扩展	256GB
视频	
视频拍摄	后置摄像头：最大支持 4K（3840×2160）视频录制 前置摄像头：最大支持 1080P 视频录制
拍摄功能	
▲后置摄像头	后置摄像：≥1600+1200+800 像素 对焦方式：激光对焦、相位对焦、反差对焦
前置摄像头	前置摄像： ≥2400 万像素
其他	
▲电池容量	≥4000mAh（典型值）
电池更换	不支持（内置不可拆卸）
快充	支持大功率快速充电
SIM 卡类型	卡槽 1：nano 卡 卡槽 2：nano 卡或超微型存储卡（NM 存储卡或 NM Card）*
其他配件	充电线、耳机、充电器、使用说明书等
设备安全检测组件要求	预装符合公安部安全监控组件

四、服务要求

1、应具备 APN/VPDN 专用通信网络，保证移动警务终端经无线传输链路到公安侧接入专线信息通信安全的能力。4G 接入速率上行速度不低于 40Mbps，下行速度不低于 150Mbps；

2、保证移动警务业务的整个通信链路不被旁路，移动警务专用 SIM/UIM 卡不能接入互联网，无线传输链路及 VPN 专线需与互联网通道进行有效隔离。

3、提供的 APN/VPDN 专用通信网络，从移动警务终端到公安侧接入专线之

间，尽量为**采购人**分配除（10/74-76）.0.0.0/8（公安信息网）、20.0.0.0/8（公安移动信息网）以外的 IP 地址网段。

4、**中标人**在**采购人**自建 LNS 服务器的前提下，为**采购人**移动警务业务中的每个移动警务终端用户分配静态 IP 地址。

5、**中标人**为**采购人**移动警务业务中使用的 APN/VPDN 域名、移动警务专用 SIM/UIM 卡数据支持全国漫游服务。

6、**采购人**移动警务业务中使用的原有 3G 专线链路升级为 4G 专线链路时，**中标人**应保证新升级链路的兼容性（兼容原有的 3G 链路，包括移动警务数据、IP 地址、协议支持等），保证用户数据的完整性及平滑过渡。

7、在**采购人**移动警务业务使用的重点区域应急处置场景下，**中标人**应尽量优先保障公安用户使用 3G/4G 数据网络，尽量优先保障公安用户的网络需要。全省市县主城区实现 4G 以上网络全覆盖；乡镇至少覆盖 3G 网络；

8、针对**采购人**用户发现的信号盲区、网络不稳定地区、网络优化需求等问题，双方协商提出解决方案，并尽快予以解决。

9、**中标人**为**采购人**移动警务业务中使用终端按需提供 LBS 定位机制，提高移动警务终端定位准确率和及时性。

10、**中标人**为**采购人**移动警务专用链路提供通信保障，有条件的情况下建议增加备用链路，实现链路冗余。

11、**中标人**为**采购人**与本地网络同级别的全国漫游网络保障。

五、管理保障要求

1、**中标人**不得对外泄露移动警务终端用户卡号信息。

2、**中标人**按要求制定项目建设管理、系统运维保障、移动警务专用 SIM/UIM 卡制发卡、售后服务保障、应急处突响应等方面的管理制度和工作流程，明确人员职责，保证各地项目建设符合移动警务相关技术规范和管理要求。

3、**中标人**在收到**采购人**提供的用户信息，并完成移动警务专用 SIM/UIM 卡入网后，应将用户信息按指定格式，以指定形式提供给公安单位，信息应包括 IMSI、ICCID、用户姓名、手机号码、归属地等项。

4、**中标人**如遇移动警务专用 SIM/UIM 卡欠费，为了不影响公安业务的开展，应及时通知公安用户本人或用户所在单位按时缴费。

5、**中标人**应做好日常网络巡检、运行分析、升级更新，出现断网故障、发现网络异常和重大网络调整等情况。应通过电话或短信第一时间通知**采购人**，迅速处置，并将处置结果及时反馈。加强节假日和重大保障时段的值班备勤，明确值守人员，随时响应和配合工作任务,对网络予以重点保障。

6、**中标人**应为**采购人**设立专门绿色通道，为**采购人**用户办理补卡（移动警务专用 SIM/UIM 卡）、换卡、查帐、交费等事宜提供方便。

7、当**采购人**需要开展系统、网络、移动警务终端等测试工作时，**中标人**应明确专班人员予以配合，并提供一定优惠、便捷政策。

8、为了保障移动警务运行安全，双方建立长效联络机制，防范安全风险，出现安全事件应及时配合**采购人**调查取证、应急处置等工作。

9、为更好支持**中标人**开展网络服务保障工作，**采购人**为**中标人**在设备安装、系统调试及信息核对等方面提供场地环境、人员配合及信息资料等必要协助。

10、**中标人**为**采购人**定制专门业务套餐，包括但不限于话费、流量包月套餐，流量池、话费池总量共享机制，集团短号内部通话套餐，0 元购警务通（两年/次）终端套餐等。

C 包采购需求

C 包采购需求

海南公安“智慧微警务”项目—监理（C 包）招标需求书

一、项目名称

海南公安“智慧微警务”项目—监理（C 包）

二、项目预算

海南公安“智慧微警务”项目—监理（C 包）预算详见第一章。

三、项目需求

3.1 监理需求部分

3.1.1 监理需求

本包监理范围为本招标文件（施工包）的建设内容。

3.1.2 监理服务周期

本项目监理服务周期自签订合同之日起，至项目终验满三年。

3.1.3 监理技术要求

3.1.3.1 监理范围

重点对项目建设过程中设备/材料的采购、设备安装调试、系统集成、软件开发及应用技术培训、试运行、测试、验收等全过程进行监督管理，从硬件监理、软件监理、系统集成监理等三个方面梳理该项目建设的工程监理应如何通过切实有效方式、方法、手段达到建设方所要求的深度、广度，最终实现工程

监理的目标。实现对质量、进度、经费、变更的控制及合同管理和文档管理。当工程质量或工期出现问题或严重偏离计划时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

根据国家网络安全法，由于本项目是重要信息基础设施，项目网络安全需要满足公安机关的信息安全等级保护要求，为了加强项目建设过程的网络安全等级保护工作，确保系统建成后通过信息安全等级保护测评，在项目各阶段重点提供如下服务：

项目前期阶段，根据《信息系统安全等级保护基本要求》（GB/T 22239-2008），辅助业主对项目的网络安全建设方案进行评审、论证。

在项目建设阶段，协助业主对系统的网络安全等级进行定级辅导，定级备案材料的编制。

在项目验收阶段，按照《信息系统安全等级保护基本要求》（GB/T 22239-2008），为业主提供包括安全策略、管理制度、操作规程等管理要求的咨询服务。

3.1.3.2 监理目标控制方案

以工程建设合同、监理委托合同、国家（GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》）及有关法规、技术规范与标准、项目建设单位需求为依据，通过专业的控制手段，协助建设单位全面地进行技术咨询和技术监督，对工程全过程进行监督、管理、指导、评价，并采取相应的组织措施、技术措施、经济措施和合同措施，确保建设行为合法、合理、科学、经济，使建设进度、投资、质量达到建设合同规定的目标。

1)、监理质量目标控制

监理质量目标控制是监理技术服务的核心所在，也是监理单位综合实力的最好反映，所以做好监理质量目标控制方案，确保本项目建设质量能达到建设单位要求的质量目标。

确保本项目建设质量达到工程合同中规定的功能、技术参数等目标。

确保工程建设中的设备和各个节点满足相关国家（GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》)、地方或行业质量标准和技术标准，按照承建合同要求进行基于总体方案的细化设计、开发、安装、调试和运行；系统集成和软件开发过程涉及用户需求调研分析、概要设计、详细设计、系统实现、系统测试和系统运行等比较复杂、制约因素多的工作内容，应该成为质量控制的重点；深化设计方案的确定、开发平台选定，也要进行充分论证。

要求监理在整个工程实施过程中做好对工程质量的事前控制，事中监督和事后评估，以确保工程质量合格。

投标人应针对本项目建设中软硬件设备采购、设备安装调试、系统集成、软件开发、工程培训等提出工程监理的质量控制原则、方法、措施、工作流程和目标。

2)、监理进度目标控制

确保本项目按合同规定的工期完工。

依据合同所约定的工期目标，在确保质量和安全的原则下，采用动态的控制方法，对进度进行主动控制，确保项目按规定的工期完工。

通过对本项目概要设计的分析、研究，提出针对本项目建设的、有代表性的信息工程监理进度控制的主要原则、方法、内容、措施、工作流程和目标。

3)、监理投资目标控制

协助用户控制本项目建设总投资在项目预算及审计范围内，减少项目建设中的额外开支。

以项目建设方和承建单位实际签订的合同金额为准，确保项目费用控制在合同规定的范围内。

在项目建设中，合理减少项目变更，保护建设单位的经济利益。

3.1.3.3 工程监理重点难点分析

投标人应根据**错误！未指定书签。**建设的特点，从实际出发分析本项目监理工作的重点、难点，并根据分析的结果制定相应的监理工作规划、对策和策略，以便日后有针对性的开展建设工程的监理服务工作。

（一）项目组织及总体技术方案的质量控制

1、协助审查项目建设方的投标书、合同及实施方案；

2、在技术上、经济上、性能上和风险上进行分析和评估，为采购人提供建议；

3、协助审查项目建设方提交的组织实施方案和项目计划等相关文档；

4、协助审查项目建设方的工程质量保证计划及质量控制体系；

5、参与制定项目质量控制的关键节点及关键路径。

（二）项目质量控制

1、组织措施：建立质量管理系统，完善职责分工及有关质量监督制度，落实质量控制责任。

2、系统集成质量控制

审核系统总集成方案；

对采购的硬件设备及网络环境的综合质量进行检验、测试和验收；

参与制定系统验收大纲；

对设备安装、调试进行验收；

对系统进行总体验收。

3、人员培训的质量控制

协助审查并确认培训计划，审定培训大纲；

监督审查建设方实施其培训计划，并征求采购人的意见反馈；

监督审查考核工作，评估培训效果；

协助审核并确认培训总结报告。

4、文档、资料的质量控制

监督审查建设方提供的设备型号、数量、到货时间以及设备的技术资料、系统集成和软件安装在实施过程中所有相关文件的标准性和规范化，在各项目验收时，应监督项目建设方提交符合规定的成套资料，包括印刷本和电子版。

对监理项目实施过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版。

（三）进度协调控制

1、组织措施：建立进度控制协调制度，落实进度控制责任。

2、编制项目控制进度计划：编制项目总进度计划和网络图。按各子系统实际情况进行编制，包括系统建设开工、设备的采购、设备的安装调试、软件的编制、试运行等各方面内容，做到既要保证各子系统、各阶段目标的顺利实现，又要保证项目间、阶段间的衔接、统一和协调。

3、审查各子系统建设方编制的工作进度计划：分析系统建设进度计划是否能满足合同工期及系统建设总进度计划的要求，特别要对照上阶段计划工程量完成情况进行审查，对为完成系统建设进度计划所采取的措施是否恰当、设备能否满足要求、管理上有无缺陷进行审查。要根据建设方所能提供的人员及设

备性能复核、计算设备能力和人员安排是否满足要求等，分析判断计划是否能落实，审查建设方提出的设备供应计划能否落实。如发现供应计划未落实，应及时报告采购人，要求建设方采取应急措施满足系统建设的需求。

4、系统建设进度的现场检查：随时或定期、全面地对进度计划的执行情况跟踪检查，发现问题及时采取有效措施加以解决。加强系统建设准备工作的检查，在工程项目或部分工序实施前，对情况进行检查，要加强检查设备、人员安排、各项措施的落实情况，确保准备工作符合要求，不影响后续工程的进行。

5、进度计划的分析与调整：要保证建设进度与计划进度一致，经常对计划进度与实际进度进行比较分析，发现实际进度与计划进度不符时，即出现进度偏差时，首先分析原因，分析偏差对后续工作的影响程度，并及时通知建设方采取措施，向建设方提出要求和修改计划的指令。

（四）投资控制

1、组织措施：建立健全项目管理组织，完善职责分工及有关质量项目管理制度，落实投资控制的责任。

2、审查设计图纸和文件，审查建设方的施工组织设计和各项技术措施，深入了解设计意图，在保证系统建设质量和安全的前提下尽可能优化设计。

3、严格督促建设方按合同实施，严格控制合同外项目的增加，协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度；及时了解系统建设情况，协调好各方矛盾，减少索赔事件的发生。对发生的事件严格按合同及法律条款进行处理，认真进行索赔调解。

（五）合同管理

合同管理是加快系统建设进度、降低系统建设造价、保证系统建设质量的有效途径之一。通过合同管理，可以督促建设方在各个阶段按照合同要求保证

设备、人员的配备及投入，保证各阶段目标按合同实施，减少索赔事件，控制系统建设结算等。具体要求如下：

1、以合同为依据，本着“实事求是、公正”的原则，合情合理地处理合同执行过程中的各种争议。

2、分析、跟踪和检查合同执行情况，确保项目建设方按时履约。

3、对合同的工期的延误和延期进行审核确认。

4、对合同变更、索赔等事宜进行审核确认。

5、根据合同约定，审核项目建设方的支付申请。

6、建立合同目录、编码和档案。

7、合同管理坚持标准化、程序化，如设计变更、延期、索赔、计量支付等应规定出固定格式和报表。合同价款的增减要有依据，合同外项目增加要严格审批制度。重大合同管理问题的处理，如大的变更、索赔、复杂的技术问题等，组成专门小组进行研究。不符合实际情况的合同条款及时向采购人报告，尽早处理，以免造成损失。

（六）信息、工程文档管理

在项目管理过程中，为了实现对进度、质量、投资的有效控制，处理有关合同管理中的各种问题，监理方需要收集各种有用的信息。信息的来源主要包括采购人文件、设计图纸和文件、建设方的文件、建设现场的现场记录（或项目管理日志）、会议记录、验收情况及备忘录等等。其中项目管理日志是进行信息管理的一个最重要的方面。项目管理日志主要包括当天的工作项目和工作内容、投入的人力和设备运行情况、计划的完成情况及进度情况、停工和返工及窝工情况。信息管理主要措施要求如下：

1、制定详细的信息收集、整理、汇总、分析、传递和利用制度，力求信息

管理的标准化和制度化。由专人负责系统建设信息的收集、分类、整理储存及传递工作。信息传递以文字为主，统一编号，利用计算机进行管理，力求信息管理的高效、迅速、及时和准确，为系统建设提供及时有用的信息和决策依据。

2、在项目实施过程中做好工程监理日记和工程大事记。

3、做好双方合同、技术建设方案、测试文档、验收报告等各类往来文件的存档。

4、建立必要的会议、例会制度，整理好会议纪要，并监督会议有关事项的执行情况。

5、立足于建设现场，加强动态信息管理，对现场的信息进行详细记录和分析，做到以文字为基础，以数据说明问题。根据收集到的信息与合同进行比较，督促建设方的人员和设备到位，促使承包商按合同完成各项目标，从而实现对进度、质量、投资的控制。

6、建立完整的各项报表制度，规范各种适合本项目的报表。定期将各种报表、信息分类汇总，及时向采购人及有关各方报送。

7、监理项目验收时，应提交符合规定的有关工程的成套资料，包括印刷本和电子版。

（七）日常监理

1. 掌握监理范围内涉及的各种技术及相关标准；

2. 安排足够的监理人员，按工程需要派驻相应的专业人员进行项目监理，至少保证 2 名专职信息系统监理工程师 5*8 小时在现场，随时为采购人提供服务，总监理工程师必需专职于本项目；

3. 制定工程管理的组织机构方案并协助采购人组建相关机构，并提供相关培训；

4. 熟悉了解项目的业务需求，协助采购人对项目的目标、范围和功能进行界定，参与并协助项目的设计方案交底审核工作；

5. 建立健全科学合理的会议制度，并予以贯彻落实；

6. 建立健全科学合理的文档管理制度,制订开发过程中产生的各类文档制作、管理规范，并予以贯彻落实；

7. 与采购方一起制定评审机制，在工程实施全过程中随时关注隐患苗头，如发现将会导致工程失败的情况出现时，应及时启动评审机制，组织专家对工程实施情况进行评审，对评审不合格的，应向采购方提出终止合同意见。此外，还应组织定期评审（阶段性评审、里程碑评审、验收评审），对评审结果为优的，提出奖励意见，评审不合格的，则向采购方提出处理意见；

3.1.3.4 工程各阶段的监理规划、实施

投标人应对本项目从设计施工到项目竣工验收阶段制定一整套工程监理的工作流程，并叙述各阶段主要监理工作内容。

本项目监理工作主要分为设备/材料采购、施工阶段、验收阶段、质保期阶段等。

⑴、设备/材料采购监理

建设项目由承包单位承担设备/材料采购任务，工程监理单位在设备/材料采购阶段监理工作主要有：

✧ 审核承包单位的设备采购计划和设备采购清单；

✧ 订货进货验证；

✧ 组织到货验收；

✧ 鉴定、设备移交等；

⑵、施工阶段监理

1、开工前的监理

1） 审核施工设计方案：开工前，由监理单位组织实施方案的审核，内容包括设计交底，了解需求、质量要求，依据设计招标文件，审核总体设计方案和有关的技术合同附件，以避免因设计失误造成实施的障碍；

2） 审核实施方案的合法性、合理性、与设计方案的符合性；

3） 审批施工组织设计：对施工单位的实施工作准备情况进行和监督；

4） 审核施工进度计划：对施工单位的施工进度计划进行评估和审查；

5） 审核实施人员:确认施工方提交的实施人员与实际工作人员的一致性，如有变更，则要求叙述其原因；

6） 审核《软件项目开发计划》。

2、施工准备阶段的监理

1） 审批开工申请，确定开工日期；

2） 了解承包商设备订单的定购和运输情况；

3） 了解施工条件准备情况；

4） 了解承建单位实施前期的人员组织、施工设备到位情况；

5） 编制各个子项目监理细则；

6） 签发开工令。

3、施工阶段的监理

1） 审核软件开发各个阶段文件；

2） 协助采购人组织软件开发阶段评审；

3） 材料、硬件设备、系统软件的供货计划的审核；

4） 材料、硬件设备、系统软件的进场、开箱和检验；

5） 促使项目中所使用的产品和服务符合合同及国家相关法律法规和标

准；

6） 对施工各个阶段的安装工艺进行检查；

7） 审核项目各个阶段进度计划；

8） 督促、检查承建单位进度执行情况；

9） 审查项目变更，提出监理意见；

10） 审查承建单位阶段款支付申请，提出监理意见；

11） 按周（月、旬）定期报告项目情况；

12） 组织召开项目例会和专项会议。

4、试运行阶段的监理

1） 协助建设方确认项目进入试运行；

2） 监查系统的调试和试运行情况，记录系统试运行数据；

3） 进行试运行期系统检测或测试，做出检测或测试报告；

4） 对试运行期间系统出现的质量问题进行记录，并责成有关单位解决。解决问题后，进行二次监测；

5） 进行试运行时间核算；

6） 协助业主确认试运行通过。

⑶、验收阶段监理

1、验收阶段

1）检查与测试是确认项目各系统所建内容是否达到合同要求和评估系统质量的必备措施，监理单位应协助建设单位明确项目测试验收方案并审查其符合性及可行性。监理机构应对项目建设的机房工程、布线等智能建筑类基础施工进行专项测试，对应用系统软件功能进行专项测试，必要时应提供或委托第三方出具国家认可实验室出具的检测报告，作为项目验收的依据。

2）对承建单位在试运行阶段出现的问题的整改情况进行监督和复查；

3）监督检查承建单位作好用户培训工作，检查用户文档；

4）组织系统初步验收；

5）审查承建单位提交的竣工文档；

6）参与项目竣工验收；

7）竣工资料收集整理齐全并装订，签署验收报告；

8）审核项目结算；

9）审查承建单位阶段款支付申请，提出监理意见；

10） 向建设单位提交监理工作总结；

11） 将所有的监理材料汇总，编制监理业务手册，提交采购人；

12） 系统验收完毕进入保修阶段的审核与签发移交证书。

2、项目移交阶段

1） 系统的设计方案、设计图纸和竣工资料的全部移交；

2） 设备、软件、材料等的验收文档核实；

3） 施工文档的移交；

4） 竣工文档的移交；

5） 项目的整体移交。

⑷、质保期阶段监理

监理单位承诺依据委托监理合同约定的工程质量保修期规定的时间、范围和内容开展工作主要有：

1） 定期对项目进行回访，协助解决技术问题；

2） 对项目建设单位提出的质量缺陷进行检查和记录；

3） 对质量缺陷原因进行调查分析并确定责任归属；

4) 检查承建单位质保期履约情况，督促执行；

5) 审查承建单位阶段款支付申请，提出监理意见。

投标人应根据上述监理工作内容（但不局限于上述内容），分别制定详细的监理工作流程，使**错误！未指定书签。**的监理工作流程化、制度化。

3.1.3.5 监理工作要求

1、监理工作制度要求

根据本项目的特色，本项目要求以现场监理为主要方式进行，在施工现场主要监理人员必须具备所从事监理业务的专业技术和类似系统经验，并具有丰富的项目管理经验。监理工作必须由具有相应资质和职称的人员来担任。本次监理项目实行总监理工程师负责制，在整个项目建设期间，总监理工程师必须保证有三分之一工作日以上的时间到甲方现场，且必须在建设期间全程常驻至少 2 名监理工程师在采购人现场。监理公司应建立项目监理小组，负责整个项目的全程监理工作，本项目必须配备不少于 3 名的现场专业工程师。监理人员的确定和变更，须事先经业主方同意。监理人员必须奉公守法，具有高度的责任心。

2、监理项目组织要求

工程监理组织形式应根据工程项目的特点、工程项目承包模式、业主委托的任务以及监理单位自身情况而确定，结构形式的选择应考虑有利于项目合同管理、有利于目标控控制、有利于决策指挥、有利于信息沟通。

要求投标人在报价方案中要明确工程监理的各项运作，包括监理人员的相关资料、职能分配、监理组织的构成及工作流程、各项监理工作的相关负责人等。

3、监理信息管理要求

投标人应制定有关本项目信息管理流程，规范各方文档并负责整理记录归档业主单位与承建单位来往的文件、合同、协议及会议记录等各种文档，并定期以监理月（周/季）报形式提交业主。包括下列监理工作：

1）做好监理日记及工程大事记；

2）做好合同批复等各类往来文件的批复和存档；

3）做好项目协调会、技术专题会等各项会议纪要；

4）管理好实施期间的各类、各方技术文档；

5）做好项目周报；

6）做好监理建议书、监理通知书存档；

7）阶段性项目总结。

投标人应针对项目特点，制定相应的信息分类表、信息流程图、信息管理表格、信息管理工作流程与措施，同时要求采用先进的项目信息管理软件对项目信息进行综合管理。

4、监理合同管理要求

本项目建设过程中会与承建单位签订各种合同，投标人应该针对项目特点制定合同从草案到签署的管理工作流程与措施，规范合同管理，并在具体项目合同执行时进行下列监理工作：

1）跟踪检查合同的执行情况，确保承建单位按时履约；

2）对合同工期的延误和延期进行审核确认；

3）对合同变更、索赔等事宜进行审核确认；

4）对合同终止进行审核确认；

5）根据合同约定，审核承建单位提交的支付申请，签发付款凭证。

要求对项目合同进行合理的管理，以完善整个项目建设的过程。

3.1.4 监理服务准则

遵照国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》的规定，以“守法、诚信、公正、科学”的准则执业，维护建设方与承建方的合法权益。具体应做到：

1） 执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责。

2） 不收受被监理单位的任何礼金。

3） 不泄漏所监理项目各方认为需要保密的事项。

4） 遵守国家的法律和政府的有关条例、规定和办法等。

5） 坚持公正的立场，独立、公正地处理有关各方的争议。

6） 坚持科学的态度和实事求是的原则。

7） 在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助被监理者完成起担负的建设任务。

8） 不泄漏所监理的项目需保密的事项。

3.1.5 监理依据

1）国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》和海南省有关信息系统项目建设和监理管理规范；

2）建设单位与承建单位签订的承包工程合同

3）建设单位与监理单位签订的委托监理合同

4）本工程招标书、招标过程文件、各中标商的投标书

5）国家有关合同、招投标、政府采购的法律法规

6）部颁、地方政府的信息工程、信息工程监理的管理办法和规定

7）建设工程和信息工程相关的国家、行业标准和规范

8）建设工程和信息工程技术监督、工程验收规范

9）与工程相关的技术资料

10）其他与本项目适用的法律、法规和标准

11）国家、地方及行业相关的技术标准

3.1.6 安全保密要求

本项目要求投标人制定一整套工程监理安全保密制度，确定工程保密责任人，同时要求投标人：

1） 按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议；

2） 监理单位各级组织严格履行保密职责；

3） 按照公司内部保密规定开展监理工作。

3.1.7 监理验收要求

1）审核监理方应提交的各类监理文档和最终监理总结报告,综合评估监理方在系统开发进度、质量把关、重难点问题解决、项目投资等方面的监理情况。只有文档齐全，系统开发工作中没有出现重大质量事故才予验收。

2）本监理工作的最终验收由委托方组织。

3.1.8 其它要求

1.监理总工程师

1）具有信息系统监理师资格证书；

2）5 年以上监理或项目管理经验。

2.监理工程师

1）具有信息系统监理师资格证书资格；

3.项目管理及施工组织

投标人须提供详尽的监理技术方案，包括但不限于施工组织部署、项目管理目标、施工准备、进度控制、质量管理、验收方法等内容。

4.系统检测能力

监理单位应具有多项检测设备及仪器，具备较为综合的网络、信息安全、软件测试能力，对本项目实施过程中的系统实施、系统测试、网络系统安全等方面能起到较高促进作用。

5.现场实施办公设施投入、监理设备

监理单位自行负责解决现场实施所需办公设备，包括现场实施所需要的 3 台移动笔记本电脑（Intel 酷睿 i7 8565U；内存 16GB LPDDR3（低功耗版）2133MHz；1TB SSD 固态硬盘；13.9 英寸屏幕尺寸；支持十点触控防指纹；NVIDIA Geforce MX250 性能级独立显卡；3000x2000 超高清屏屏幕分辨率）并严格按照入网管理专机专用。项目建设结束后，由采购方按照相关工作要求技术检测和处理，确保设备中无相关敏感信息存储内容后返还。